D-Link DES-3500 シリーズ

Layer2 Managed Stackable Fast Ethernet Switch

コマンドラインインタフェース (CLI) マニュアル

ご注意

本書は、コマンドラインインタフェースの説明および設定方法を記載しています。本シリーズの仕様、設置方法など使用するために必要な基本的な取り扱い方法については、設置マニュアルおよびユーザマニュアルをご覧ください。

D-Link®
Building Networks for People

安全にお使いいただくために

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠警告	この表示を無視し、まちがった使いかたをすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、まちがった使いかたをすると、傷害または物損損害が発生するおそれがあります。

記号の意味　⃠ してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠警告

分解禁止　**分解・改造をしない**
機器が故障したり、異物が混入すると、やけどや火災の原因となります。

禁止　**落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない**
故障の原因につながります。

禁止　**発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない**
感電、火災の原因になります。
使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼してください。

ぬれ手禁止　**ぬれた手でさわらない**
感電のおそれがあります。

水ぬれ禁止　**水をかけたり、ぬらしたりしない**
内部に水が入ると、火災、感電、または故障のおそれがあります。

禁止　**油煙、湯気、湿気、ほこりの多い場所、振動の激しいところでは使わない**
火災、感電、または故障のおそれがあります。

禁止　**内部に金属物や燃えやすいものを入れない**
火災、感電、または故障のおそれがあります。

禁止　**表示以外の電圧で使用しない**
火災、感電、または故障のおそれがあります。

禁止　**たこ足配線禁止**
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

禁止　**設置、移動のときは電源プラグを抜く**
火災、感電、または故障のおそれがあります。

禁止　**雷鳴が聞こえたら、ケーブル / コード類にはさわらない**
感電のおそれがあります。

禁止　**ケーブル / コード類や端子を破損させない**
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障につながります。

禁止　**正しい電源ケーブル、コンセントを使用する**
火災、感電、または故障の原因となります。

禁止　**乳幼児の手の届く場所では使わない**
やけど、ケガ、または感電の原因になります。

禁止　**次のような場所では保管、使用をしない**
・直射日光のあたる場所
・高温になる場所
・動作環境範囲外

禁止　**光源をのぞかない**
光ファイバケーブルの断面、コネクタ、および製品のコネクタをのぞきますと強力な光源により目を損傷するおそれがあります。

⚠注意

❗　**静電気注意**
コネクタやプラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。

❗　**コードを持って抜かない**
コードを無理に曲げたり、引っ張りますと、コードや機器の破損の原因となります。

❗　**振動が発生する場所では使用しない**
接触不良や動作不良の原因となります。

禁止　**付属品の使用は取扱説明書にしたがう**
付属品は取扱説明書にしたがい、他の製品には使用しないでください。機器の破損の原因になります。

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。
この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。
この場合には使用者が適切な対策を講ずるよう要求されることがあります。

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、ユーザマニュアルおよび同梱されている製品保証書をよくお読みいただき、内容をご理解いただいた上で、記載事項にしたがってご使用ください。

- 本書および同梱されている製品保証書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 本書および同梱されている製品保証書は大切に保管してください。
- 弊社製品を日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
また、テクニカルサポートご提供のためにはユーザ登録が必要となります。
http://www.dlink-jp.com/

目次

安全にお使いいただくために 2

第 1 章　はじめに 14

シリアルポート経由でスイッチに接続する 14
スイッチの IP アドレス設定 15

第 2 章　コンソール CLI を使用する 16

スイッチに接続する 16

第 3 章　コマンド構文 19

第 4 章　基本のスイッチコマンド 21

create account 22
config account 23
show account 23
delete account 24
show session 24
show switch 25
show serial_port 26
config serial_port 26
enable clipaging 27
disable clipaging 27
enable telnet 27
disable telnet 28
enable web 28
disable web 28
save 29
reboot 29
reboot force_agree 29
reset 30
login 30
logout 31
config command_prompt 31
config greeting_message 32
show greeting_message 33
telnet 33
enable greeting_message 34
disable greeting_message 34

第 5 章　スイッチポートコマンド 35

config ports 35
show ports 36

第 6 章　ポートセキュリティコマンド 37

config port_security ports 37
delete port_security_entry 38
clear port_security_entry 38
show port_security 39
enable port_security trap_log 39
disable port_security trap_log 40

第 7 章　ネットワーク管理（SNMP）コマンド 41

create snmp user 42
delete snmp user 43
show snmp user 43
create snmp view 44
delete snmp view 44
show snmp view 45
create snmp community 46
delete snmp community 46
show snmp community 47
config snmp engineID 47
show snmp engineID 48

create snmp group 48
delete snmp group 49
show snmp groups 50
create snmp host 51
delete snmp host 51
show snmp host 52
create trusted_host 52
create trusted_host network 53
delete trusted_host ipaddr 53
delete trusted_host network 54
delete trusted_host all 54
show trusted_host 55
enable snmp traps 55
enable snmp authenticate traps 56
show snmp traps 56
disable snmp traps 56
disable snmp authenticate traps 57
config snmp system_contact 57
config snmp system_location 58
config snmp system_name 58
enable rmon 59
disable rmon 59

第 8 章　スイッチユーティリティコマンド（ファイルシステムコマンドを含む） 60

download 61
upload 62
config firmware image_id 63
show config 63
ping 64
enable autoconfig 65
disable autoconfig 66
show autoconfig 66
show firmware information 67

第 9 章　ネットワークモニタリングコマンド 68

show packet ports 69
show error ports 69
show utilization 70
clear counters 71
clear log 71
show log 72
enable syslog 72
disable syslog 72
show syslog 73
create syslog host 73
config syslog host 74
delete syslog host 75
show syslog host 75
config system_severity 76
show system_severity 77

第 10 章　マルチプルスパニングツリー（MSTP）コマンド 78

enable stp 79
disable stp 79
config stp version 79
config stp 80
config stp ports 81
create stp instance_id 82
config stp instance_id 82
delete stp instance_id 83
config stp priority 84
config stp mst_config_id 84
config stp mst_ports 85

show stp 86
show stp ports 87
show stp instance_id 87
show stp mst_config_id 88

第 11 章　フォワーディングデータベースコマンド 89

create fdb 89
create multicast_fdb 90
config multicast_fdb 90
config fdb aging_time 91
delete fdb 91
clear fdb 92
show multicast_fdb 92
show fdb 93
config multicast port_flitering_mode 94
show multicast port_filtering_mode 94

第 12 章　トラフィックコントロールコマンド 95

config traffic control 96
config traffic control_trap 97
show traffic control 98

第 13 章　QoS コマンド 99

config bandwidth_control 99
show bandwidth_control 100
config scheduling 101
show scheduling 102
config 802.1p user_priority 102
show 802.1p user_priority 103
config 802.1p default_priority 103
show 802.1p default_priority 104

第 14 章　ポートミラーリングコマンド 105

config mirror port 105
enable mirror 106
disable mirror 106
show mirror 107

第 15 章　VLAN コマンド 108

create vlan 108
delete vlan 109
config vlan 109
config gvrp 110
enable gvrp 110
disable gvrp 111
show vlan 111
show gvrp 112

第 16 章　Asymmetric VLAN コマンド 113

enable asymmetric_vlan 113
disable asymmetric_vlan 113
show asymmetric_vlan 114

第 17 章　リンクアグリゲーションコマンド 115

create link_aggregation group_id 115
delete link_aggregation group_id 116
config link_aggregation group_id 116
config link_aggregation algorithm 117
show link_aggregation 117
config lacp_port 118
show lacp_port 119

第 18 章　IP-MAC-Port バインディング（IMPB）コマンド 120

create address_binding ip_mac ipaddress 121
config address_binding ip_mac ipaddress 122
config address_binding ip_mac ports 122
show address_binding 123
delete address_binding 123
enable address_binding acl_mode 124
disable address_binding acl_mode 124
enable address_binding trap_log 125
disable address_binding trap_log 125

第 19 章　基本 IP コマンド 126

config ipif 126
show ipif 127

第 20 章　IGMP Snooping コマンド 128

config igmp_snooping 128
config router_ports 129
config router_ports_forbidden 129
enable igmp_snooping 130
disable igmp_snooping 130
show igmp_snooping 131
show igmp_snooping group 132
show router_ports 132
show igmp_snooping forwarding 133
create igmp_snooping multicast_vlan 133
config igmp_snooping multicast_vlan 134
delete igmp_snooping multicast_vlan 134
show igmp_snooping multicast_vlan 135

第 21 章　DHCP リレーコマンド 136

config dhcp_relay 136
config dhcp_relay add ipif 136
config dhcp_relay delete ipif 137
config dhcp_relay option_82 state 137
config dhcp_relay option_82 check 138
config dhcp_relay option_82 policy 138
show dhcp_relay 139
enable dhcp_relay 139
disable dhcp_relay 140

第 22 章　IP マルチキャスト範囲の限定コマンド 141

create multicast_range 141
delete multicast_range 141
show multicast_range 142
config limited multicast address 142
show limited multicast address 143

第 23 章　802.1X コマンド 144

enable 802.1x 145
disable 802.1x 145
show 802.1x auth_configuration 146
show 802.1x auth_state 147
config 802.1x auth_mode 148
config 802.1x capability ports 149
config 802.1x auth_parameter ports 149
config 802.1x auth_protocol 150
config 802.1x init 150
config 802.1x reauth 151
config radius add 151
config radius delete 152

config radius 152
show radius 153
create 802.1x guest_vlan 153
config 802.1x guest_vlan ports 154
show 802.1x guest_vlan 154
delete 802.1x guest_vlan 155

第 24 章　アクセスコントロールリスト（ACL）コマンド 156

create access_profile（for Ethernet） 158
config access_profile_id（for Ethernet） 159
create access_profile（IP） 160
config access_profile（IP） 161
create access_profile（packet content） 162
config access_profile（packet content） 163
create access_profile（ipv6） 164
config access_profile（ipv6） 164
delete access_profile 165
show access_profile 166
enable cpu_interface_filtering 166
disable cpu_interface_filtering 167
create cpu access_profile 167
config cpu access_profile 169
delete cpu access_profile 170
show cpu access_profile 171

第 25 章　SNTP 設定コマンド 172

config sntp 172
show sntp 173
enable sntp 173
disable sntp 174
config time 174
config time_zone 175
config dst 175
show time 176

第 26 章　セーフガードエンジンコマンド 177

config safeguard_engine 178
show safeguard_engine 178

第 27 章　フィルタコマンド 179

config filter dhcp_server 180
show filter dhcp_server 181
config filter netbios 181
show filter netbios 182
config filter extensive_netbios 182
show filter extensive_netbios 183

第 28 章　トラフィックセグメンテーションコマンド 184

config traffic_segmentation 184
show traffic_segmentation 185

第 29 章　ARP コマンド 186

create arpentry 186
config arpentry 186
delete arpentry 187
show arpentry 187
config arp_aging time 188
clear arptable 188

第 30 章　ルーティングテーブルコマンド 189

create iproute 189
delete iproute 189
show iproute 190

第 31 章　MAC 通知コマンド 191

enable mac_notification 191
disable mac_notification 191
config mac_notification 192
config mac_notification ports 192
show mac_notification 193
show mac_notification ports 193

第 32 章　アクセス認証コントロールコマンド 194

enable authen_policy 195
disable authen_policy 196
show authen_policy 196
create authen_login method_list_name 196
config authen_login 197
delete authen_login method_list_name 198
show authen_login 198
create authen_enable method_list_name 199
config authen_enable 199
delete authen_enable method_list_name 200
show authen_enable 200
config authen application 201
show authen application 201
create authen server_group 202
config authen server_group 202
delete authen server_group 203
show authen server_group 203
create authen server_host 204
config authen server_host 205
delete authen server_host 205
show authen server_host 206
config authen parameter response_timeout 206
config authen parameter attempt 207
show authen parameter 207
enable admin 208
config admin local_enable 208

第 33 章　SSH コマンド 209

enable ssh 209
disable ssh 210
config ssh authmode 210
show ssh authmode 211
config ssh server 211
show ssh server 212
config ssh user 212
show ssh user authmode 213
config ssh algorithm 214
show ssh algorithm 215
config ssh regenerate hostkey 216

第 34 章　SSL コマンド 217

enable ssl 218
disable ssl 219
config ssl cachetimeout 219
show ssl cachetimeout 220
show ssl 220
download certificate_fromTFTP 221

第 35 章　ループバック検知コマンド 222

config loopdetect 222
config loopdetect ports 223
enable loopdetect 223
disable loopdetect 224
show loopdetect 224
show loopdetect ports 225

第 36 章　D-Link シングル IP マネジメントコマンド 226

バージョン 1.6 へのアップグレード 227
enable sim 227
disable sim 227
show sim 228
reconfig 230
config sim_group 230
config sim 231
download sim 232
upload sim_ms 233

第 37 章　コマンドヒストリリストコマンド 234

? 234
config command_history 235
show command_history 235
dir 236

第 1 章　はじめに

xStack DES-3500 シリーズは D-Link xStack スイッチファミリーのメンバです。xStack は、エッジの 10/100Mbps スイッチからコアのギガビットスイッチまでサポートするスタッカブルスイッチのファミリーです。xStack は高性能、フォルトトレランス、スケーラブルな柔軟性、強健なセキュリティ、標準規格に準拠した相互運用性をサポートしており、将来的な部門ネットワークおよびエンタプライズネットワーク構築への移行も簡単に行うことができます。本スイッチは、シリアルポート、Telnet、または Web ベースマネジメントエージェントを通してスイッチの管理を行うことができます。本マニュアルでは CLI に含まれるコマンドに関して説明しています。Web ベースマネジメントエージェントを経由したスイッチ設定および管理については、ユーザマニュアルに記載しています。

シリアルポート経由でスイッチに接続する

スイッチのシリアルポートの設定は以下の通りです。

- データ速度 : 9600 ビット / 秒
- パリティ : なし
- データビット : 8
- ストップビット : 1
- フロー制御 : なし
- エミュレーションモード : VT100
- ファンクションキー、方向キー、Ctrl キーの使い方 : ターミナルキー

VT-100 端末をエミュレート可能な端末ソフトが動作し、上記シリアルポート設定を行っているコンピュータを RS-232（D-Sub 9 ピン）ケーブルでスイッチのシリアルポートに接続します。
シリアルポートが適切に管理コンピュータに接続されると、以下の画面が表示されます。表示されない場合、Ctrl+R を押し、コンソール画面を更新してください。

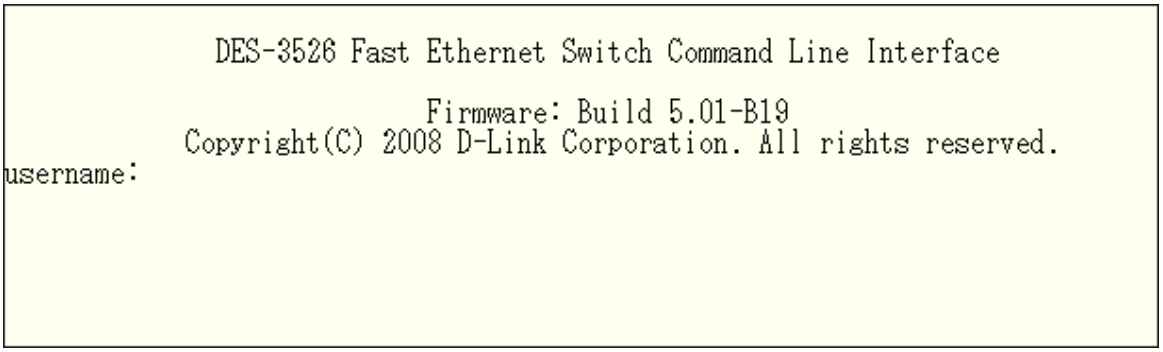

図 1-1　　初期の CLI 画面

本製品にはユーザ名とパスワードの初期値はありません。入力プロンプトに対して、 2 回「Enter」キーを押すと、「DES-35xx: admin #」が表示されます。これは、すべてのコマンドを入力する場合のコマンドプロンプトです。

スイッチの IP アドレス設定

各スイッチに対して、SNMP ネットワークマネージャまたは他の TCP/IP アプリケーション（例 :BOOTP、TFTP）と通信するために IP アドレスを割り当てる必要があります。本スイッチの IP アドレスの初期値は「10.90.90.90」です。この IP アドレスはご使用のネットワークのアドレス計画に基づいて変更することができます。
また、本スイッチには、出荷時に固有の MAC アドレスが割り当てられています。本 MAC アドレスを変更することはできません。初期起動時のコンソール画面に表示されます。

```
 Boot Procedure                                                    3.00.008
--------------------------------------------------------------------------------
 Power On Self Test ..................................... 100 %

 MAC Address   : 00-19-5B-7D-4F-F1
 H/W Version   : 0A3G

 Please wait, loading V5.01-B19 Runtime image .............  00 %
```

図 1-2　起動画面

本スイッチの MAC アドレスは、Web ベース管理インタフェースの「Administration」メニューの「Device Information」画面にも表示されます。
本スイッチの IP アドレスは、Web ベース管理インタフェースの使用前に設定する必要があります。スイッチの IP アドレスは、BOOTP または DHCP プロトコルを使用して自動的に取得することもできます。この場合は、スイッチに割り当てた本来のアドレスを知っておく必要があります。
IP アドレスはコンソールから CLI を使用して、以下のように設定することができます。

1. **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**
   xxx.xxx.xxx.xxx は IP アドレスを示し、「System」と名づけた IP インタフェースに割り当てられます。
2. または、**config ipif System ipaddress xxx.xxx.xxx.xxx/z** と入力することもできます。
   yyy.yyy.yyy.yyy/z は対応するサブネットマスクを示しています。**xxx.xxx.xxx.xxx** は IP インタフェースに割り当てられた IP アドレスを示し、**z** は CIDR 表記で対応するサブネット数を表します。

本スイッチ上の「System」という名前の IP インタフェースに IP アドレスとサブネットマスクを割り当てて、管理ステーションから本スイッチの Telnet または Web ベースの管理エージェントに接続します。

```
            DES-3526 Fast Ethernet Switch Command Line Interface

                          Firmware: Build 5.01-B19
          Copyright(C) 2008 D-Link Corporation. All rights reserved.
username:
password:

DES-3526:admin#config ipif System ipaddress 10.24.22.200/255.255.255.0
Command: config ipif System ipaddress 10.24.22.200/24

Success.

DES-3526:admin#
```

図 1-3　IP アドレスの割り当て

上記例では、スイッチに IP アドレス「10.24.22.200」とサブネットマスク「255.0.0.0」を割り当てています。「Success.」というメッセージにより、コマンドの実行が成功したことが確認できます。スイッチのアドレス設定が終了すると、Telnet、SNMP MIB ブラウザおよび CLI 経由、または上記 IP アドレスを使用した Web ベース管理エージェントによる設定と管理を開始することができます。

第 2 章　コンソール CLI を使用する

スイッチはコンソール管理インタフェースをサポートしており、シリアルポートと端末エミュレーションプログラムが動作する端末またはコンピュータを経由してスイッチの管理エージェントに接続できます。また、ネットワーク上で TCP/IP Telnet プロトコルを使用してコンソールを使用することができます。コンソールプログラムは、ネットワーク上で SNMP ベースのネットワーク管理ソフトウェアを使用するためにスイッチに設定されます。
本章ではコンソールを使用してスイッチに接続し、設定の変更および操作のモニタを行う方法について説明します。

注意　スイッチコンフィグレーション設定は、「save」コマンドを使用して NV-RAM に保存されます。現在の設定は、スイッチが再起動されると、スイッチの NV-RAM に保持され、リロードされます。「save」コマンドを使用してない再起動すると、最後に保存された設定が NV-RAM に書き込まれます。

スイッチに接続する

コンソールインタフェースは、RS-232C シリアルケーブルを使用して VT-100 互換端末または通常の端末エミュレータプログラム（例 : Windows OS に搭載のハイパーターミナル）が動作するコンピュータにスイッチを接続して使用します。端末には以下のパラメータを設定します。

- エミュレーションモード : VT-100
- データ速度 : 9600 ビット / 秒
- データビット : 8
- パリティ : なし
- ストップビット : 1
- フロー制御 : なし

さらに、Telnet インタフェースを経由して同じ機能に接続することもできます。スイッチに IP アドレスを設定すると、Telnet プログラム（VT-100 モード）を使用し、スイッチに接続して制御することができます。コンソールポートまたは Telnet インタフェースのどちらから接続しても同じ画面が表示されます。
スイッチが再起動し、ログインすると、以下のコンソール画面が表示されます。

```
            DES-3526 Fast Ethernet Switch Command Line Interface

                              Firmware: Build 5.01-B19
          Copyright(C) 2008 D-Link Corporation. All rights reserved.
username:
password:

DES-3526:admin#
```

図 2-1　　ログイン後の初期コンソール画面

コマンドを「**DES-3800:admin#**」というコマンドプロンプトの後に入力します。

CLI には多くの便利な機能があります。「**?**」コマンドを入力すると、トップレベルの全コマンドリストが表示されます。

```
DES-3526:admin#?
Command: ?


..
?
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear fdb
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config address_binding dhcp_snoop max_entry ports
config address_binding ip_mac ipaddress
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

図 2-2　「?」コマンド

必須パラメータなしでコマンドを入力すると、CLI は「**Next possible completions**」メッセージを表示します。

```
DES-3526:admin#config account
Command: config account

Next possible completions:
<username>

DES-3526:admin#
```

図 2-3　コマンドパラメータヘルプ例

この場合、「config account」コマンドには <username> パラメータが入力されます。CLI は、「**Next possible completions**」メッセージで <username> の入力を促します。CLI のすべてのコマンドには本機能があり、複雑なコマンドは、複数のパラメータ階層で入力を促します。
さらに、どんなコマンドも 1 スペースを付けて入力すると、引き続き、「Tab」キーを押すことで次に可能なサブコマンドのすべてを参照することができます。

コマンドプロンプトで前のコマンドを再入力するためには、矢印キーを押します。前のコマンドがコマンドプロンプトに表示されます。

```
DES-3526:admin#config account
Command: config account

Next possible completions:
<username>

DES-3526:admin#config account
```

図 2-4　上矢印キーを使用したコマンドの再入力

上記の例では、「config account」コマンドは必須パラメータの <username> なしで入力したため、CLI は「**Next possible completions**」を返しています。<username> プロンプトで上矢印カーソルキーを入力して、コマンドプロンプトでは前のコマンド（config account）を入力しています。適切なユーザ名が入力すると、「config account」コマンドが再実行されます。
CLI のすべてのコマンドがこのように動作します。さらに、ヘルププロンプトの構文は、本マニュアルで提供されるものと同じです。< > は数値または文字列、{} はオプションパラメータまたはパラメータの選択、[] は必須パラメータを示します。
CLI で認識されていないコマンドを入力すると、トップレベルのコマンドが以下の通り表示されます。

```
DES-3526:admin#the

Available commands:
..                  ?                   clear               config
create              delete              dir                 disable
download            drv                 enable              login
logout              ping                reboot              reconfig
reset               save                show                telnet
upload

DES-3526:admin#
```

図 2-5　利用可能なコマンド

トップレベルのコマンドは「show」または「config」などがあります。これらのコマンドの多くは、トップレベルのコマンドを限定するために 1 つ以上のパラメータを必要とします。「show xxx?」または「config xxx?」とします。「xxx?」が次のパラメータです。
例えば、「show」コマンドを付加パラメータなしで入力すると、CLI は次に可能なパラメータのすべてを表示します。

```
DES-3526:admin#create
Command: create

Next possible completions:
802.1x              access_profile      account             address_binding
arpentry            authen              authen_enable       authen_login
cpu                 fdb                 igmp_snooping       iproute
link_aggregation    multicast_fdb       multicast_range     snmp
stp                 syslog              trusted_host        vlan

DES-3526:admin#
```

図 2-6　Next possible completions - create コマンド

上記例では、「create」コマンドの次に入力可能なパラメータのすべてが表示されています。

第 3 章　コマンド構文

以下の記号は、本マニュアルにおけるコマンドエントリの記述、および値と引数の指定を説明するために使用されます。CLI に含まれ、コンソールインタフェース経由で利用可能なオンラインヘルプは同じ構文を使用します。

注意　すべてのコマンドが大文字、小文字を区別します。大文字、小文字を変更する「Caps Lock」または他の不要な機能を無効にしてください。

注意　本章で紹介されているコマンドはあくまでも例文です。実際のコマンド、構文、説明、使用例については 4 章以降の説明をご覧ください。

< 山括弧 >

目的

指定の必要がある変数または値を囲みます。

構文

create account [admin | user] <username 15>

説明

上の構文例では、<username> にユーザ名を入力する必要があります。< > は入力しません。

使用例

create account admin newadmin1

[角括弧]

目的

必要な値または引数を囲みます。値または引数を指定します。

構文

create account [admin | user] <username 15>

説明

上の構文例では、アカウントを作成するために「admin」または「user」レベルのいずれかを指定する必要があります。[ ] は入力しません。

使用例

create account user newuser1

| 垂直線

目的

リスト内の 2 つ以上の排他的な項目を分けて、そのうちの 1 つを入力する必要があります。

構文

create account [admin | user] <username 15>

説明

上の構文例では、「admin」または「user」を指定する必要があります。垂直線は入力しません。

使用例

create account user newuser1

{ 中括弧 }

目的

オプションの値かオプションの引数を囲みます。

構文

reset {[config | system]}

説明

上の構文例では、「config」または「system」を指定するオプションがあります。オプションの値を指定する必要はありませんが、システムリセットの効果は指定される値に依存します。そのため、この例では、システムリセットの実行によって 3 つの結果があります。リセットコマンドに関する詳細に関しては、「第 4 章 基本のスイッチコマンド」を参照してください。

使用例

reset config

行編集キーの使い方

表 3-1　行編集キー

キー	説明
Delete キー	カーソル下の文字を削除して、次に、ラインで残っている文字を左にシフトします。
Backspace キー	文字をカーソルの左方向に削除して、次に、ラインで残っている文字を左にシフトします。
Insert キーまたは Ctrl+R	オンとオフを切り替えます。オンの場合、文字を挿入し、前の文字を右にシフトします。
左矢印キー	左にカーソルを移動します。
右矢印キー	右にカーソルを移動します。
上矢印キー	前に入力したコマンドを繰り返します。上矢印キーが押されるたびに表示されているものよりも前のコマンドが表示されます。このように、現在のセッションのコマンドヒストリを見直すことができます。コマンドヒストリリストを順番に追って前に進めるためには、下矢印キーを使用します。
下矢印キー	下矢印キーは現在のセッションに入力されたコマンドヒストリにおいて次のコマンドを表示します。入力した通りに、各コマンドは連続して表示されます。上矢印キーを使用して、前のコマンドを見直します。
Tab キー	左にある次のフィールドにカーソルをシフトします。

ページ表示制御キー

表 3-2　ページ表示制御キー

キー	説明
スペースキー	次のページを表示します。
CTRL+C キー	複数のページが表示される場合、残りのページの表示を止めます。
ESC キー	複数のページが表示される場合、残りのページの表示を止めます。
n	次のページを表示します。
p	前のページを表示します。
q	複数のページが表示される場合、残りのページの表示を止めます。
r	現在表示されているページを更新します。
a	ページ表示を中断せずに、残りのページを表示します。
Enter キー	次の行またはテーブルエントリを表示します。

第 4 章　基本のスイッチコマンド

コマンドラインインタフェース（CLI）における基本的なスイッチコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create account	[admin | operator | user] <username 15>
config account	<username 15>
show account	
delete account	[<username 15> | <username 15> force_agree]
show session	
show switch	
show serial_port	
config serial_port	{baud_rate [9600 | 19200 | 38400 | 115200] auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}
enable clipaging	
disable clipaging	
enable telnet	<tcp_port_number 1-65535>
disable telnet	
telnet	<ipaddr> {tcp_port <value 0-65535>}
enable web	<tcp_port_number 1-65535>
disable web	
save	
reboot	
reboot	force_agree
reset	{[config | system]}
reset	{[config force_agree | system force_agree]}
login	
logout	
config command_ prompt	[<string 16> | username | default]
config greeting_message	{default}
show greeting_message	
enable greeting_message	
disable greeting_message	

次のセクションから各コマンドについて詳しく記述します。

create account

目的

ユーザアカウント作成します。

構文

create account [admin | operator | user] <username 15>

説明

ユーザアカウントを作成します。8 個までのユーザアカウントを作成できます。

パラメータ

パラメータ	説明
admin <username 15>	スイッチにすべての権利を持ってアクセスできる「admin」ユーザ（半角英数字 15 文字以内）を作成します。管理者権限のユーザだけがこのコマンドを実行できます。
operator <username 15>	スイッチに一部制限のある権利でアクセスするユーザ（半角英数字 15 文字以内）を作成します。
user <username 15>	スイッチに一部の権利でアクセスするユーザ（半角英数字 15 文字以内）を作成します。

制限事項

管理者レベルユーザだけが本コマンドを実行できます。

使用例

「dlink」というユーザ名で管理者レベルのユーザアカウントを作成します。

```
DES-3526:admin#create account admin dlink
Command: create account admin dlink

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DES-3526:admin#
```

「frazier」というユーザ名でオペレータレベルのユーザアカウントを作成します。

```
DES-3526:admin#create account operator frazier
Command: create account operator frazier

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DES-3526:admin#
```

「reed」というユーザ名でユーザレベルのユーザアカウントを作成します。

```
DES-3526:admin#create account user reed
Command: create account user reed

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DES-3526:admin#
```

config account

目的

ユーザアカウントを設定します。

構文

config account <username>

説明

「create account」コマンドで作成したユーザアカウントを設定します。

パラメータ

パラメータ	説明
<username>	パスワードを変更するアカウントの新しいユーザ名（半角英数字 15 文字以内）を入力します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

「dlink」というアカウントのユーザパスワードを設定します。

```
DES-3526:admin#config account dlink
Command: config account dlink

Enter a old password:****
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DES-3526:admin#
```

show account

目的

ユーザアカウントを表示します。

構文

show account

説明

スイッチに作成済みのすべてのユーザアカウントを表示します。8 個までのユーザアカウントを表示します。

パラメータ

なし。

制限

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチに作成済みのすべてのユーザアカウントを表示します。

```
DES-3526:admin#show account
Command: show account

Current Accounts:
Username        Access Level
--------        ------------
dlink           Admin

DES-3526:admin#
```

delete account

目的

設定済みのユーザアカウントを削除します。

構文

delete account [<username> | <username> force_agree]

説明

「create account」コマンドを使用して作成したユーザアカウントを削除します。

パラメータ

パラメータ	説明
<username>	削除するユーザアカウント名を入力します。
<username> force_agree	強制的に削除するユーザーアカウント名を削除します。

制限

管理者レベルユーザのみ本コマンドを実行できます。

使用例

「System」というユーザアカウントを削除します。

```
DES-3526:admin#delete account System
Command: delete account System

Are you sure to delete the last administrator account?(y/n)
Success.

DES-3526:admin#
```

最後の管理者アカウントを削除する場合には、「Are you sure to delete the last administrator account? (y/n)」という確認メッセージが表示されます。削除する場合には、「y」、削除しない場合には「n」を入力します。

show session

目的

現在ログインしているユーザのリストを表示します。

構文

show session

説明

コマンドを実行した際にログインしているすべてのユーザのリストを表示します。

パラメータ

なし

制限事項

なし。

使用例

ユーザのログイン方法を表示します。

```
DES-3526:admin#show session
Command: show session

ID  Login Time           Live Time     From              Level  Name
--  -------------------  ------------  ---------------  -----  ---------------
*8  2008/08/06 10:21:54  0:18:26.440   Serial Port       5      Anonymous

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

show switch

目的

スイッチに関する一般的な情報を表示します。

構文

show switch

説明

スイッチに関する情報を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに関する情報を表示します。

```
DES-3526:admin#show switch
Command: show switch

Device Type        : DES-3526 Fast-Ethernet Switch
Combo Port Type    : 1000Base-T + 1000Base-T
MAC Address        : 00-19-5B-7D-4F-F1
IP Address         : 10.90.90.90 (Manual)
VLAN Name          : default
Subnet Mask        : 255.0.0.0
Default Gateway    : 0.0.0.0
Boot PROM Version  : Build 3.00.008
Firmware Version   : Build 5.01-B19
Hardware Version   : 0A3G
Device S/N         :
Power Status       : Main - Normal, Redundant - Not Present
System Name        :
System Location    :
System Contact     :
Spanning Tree      : Disabled
GVRP               : Disabled
IGMP Snooping      : Disabled
TELNET             : Disabled
SSH                : Disabled
WEB                : Disabled
RMON               : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All

DES-3526:admin#
```

show serial_port

目的

現在のシリアルポート設定を表示します。

構文

show serial_port

説明

現在のシリアルポート設定を表示します。

パラメータ

なし。

制限事項

なし

使用例

シリアルポート設定を表示します。

```
DES-3526:admin#show serial_port
Command: show serial_port

Baud Rate   : 9600
Data Bits   : 8
Parity Bits : None
Stop Bits   : 1
Auto-Logout : 10 mins

DES-3526:admin#
```

config serial_port

目的

シリアルポートを設定します。

構文

config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}

説明

シリアルポートのボーレートおよび自動ログアウト機能を設定します。

パラメータ

パラメータ	説明
baud_rate [9600 | 19200 | 38400 | 115200]	管理ホストと通信を行うために使用されるシリアルボーレート。次の 4 つのオプションがあります。9600、19200、38400、115200。
auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]	自動的にログアウトする時間を設定します。 • never - コンソールはユーザからの入力がなくなってもオープンにしておく時間を制限しません。 • 2_minutes - コンソールはユーザからの入力がなくなってから、2 分経過するとログアウトします。 • 5_minutes - コンソールはユーザからの入力がなくなってから、5 分経過するとログアウトします。 • 10_minutes - コンソールはユーザからの入力がなくなってから、10 分経過するとログアウトします。 • 15_minutes - コンソールはユーザからの入力がなくなってから、15 分経過するとログアウトします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ボーレートを設定します。

```
DES-3526:admin#config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

DES-3526:admin#
```

enable clipaging

目的

「show」コマンドが 1 ページ以上を表示する時、コンソール画面のスクロールを一時停止します。

構文

enable clipaging

説明

コンソール画面で「show」コマンドにより複数ページがすぐにスクロールしてしまう場合に使用します。本コマンドは、ページごとに一時停止します。初期値は有効です。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

「show」コマンド出力がページの終わりに到達すると画面表示は一時停止します。

```
DES-3526:admin#enable clipaging
Command: enable clipaging
Success.

DES-3526:admin#
```

disable clipaging

目的

「show」コマンドが 1 ページ以上を表示する時、コンソール画面のスクロールを一時停止する機能を無効にします。

構文

disable clipaging

説明

「show」コマンドが複数ページに渡る情報を表示する場合に各ページの終わりでコンソール画面を一時停止する機能を無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

コマンド出力がページの終わりに達する場合に、画面表示を一時停止する機能を無効にします。

```
DES-3526:admin#disable clipaging
Command: disable clipaging
Success.

DES-3526:admin#
```

enable telnet

目的

Telnet プロトコルを使用したスイッチとの通信および管理を有効にします。

構文

enable telnet {<tcp_port_number 1-65535>}

説明

本コマンドは、スイッチの Telnet プロトコルを有効にします。スイッチが Telnet リクエストをリスニング（受信）するために使用する TCP または UDP ポート番号を指定します。

パラメータ

パラメータ	説明
{<tcp_port_number 1-65535>}	TCP ポート番号。TCP ポート番号は 1-65535 です。Telnet プロトコルの一般的な TCP ポート番号は 23 です。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

Telnet を有効にし、ポート番号を設定します。

```
DES-3526:admin#enable telnet 23
Command: enable telnet 23
Success.

DES-3526:admin#
```

disable telnet

目的

スイッチの Telnet プロトコルを無効にします。

構文

disable telnet

説明

スイッチの Telnet プロトコルを無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチの Telnet プロトコルを無効にします。

```
DES-3526:admin#disable telnet
Command: disable telnet

Success.

DES-3526:admin#
```

telnet

目的

ネットワーク上の別の機器に接続します。

構文

telnet <ipaddr> {tcp_port <value 0-65535>}

説明

ネットワーク上の別の機器に接続して設定をします。

パラメータ

パラメータ	説明
<Ipaddr>	接続する機器の IP アドレスを設定します。
tcp_port <value 0-65535>	TCP ポート番号。TCP ポート番号は 1-65535 です。Telnet プロトコルの一般的な TCP ポート番号は 23 です。

制限事項

管理者レベルおよびオペレータレベルユーザだけが本コマンドを実行できます。

使用例

ネットワーク上の別の機器に接続します。

```
DES-3526:admin#telnet 10.53.13.99 tcp_port 23
Command: telnet 10.53.13.99 tcp_port 23

Success.

DES-3526:admin#
```

enable web

目的

スイッチの HTTP ベースの管理ソフトウェアを有効にします。

構文

enable web {<tcp_port_number 1-65535>}

説明

スイッチの Web ベースの管理ソフトウェアを有効にします。スイッチが Telnet リクエストをリスニング（受信）するために使用する TCP ポート番号を指定します。

パラメータ

パラメータ	説明
{<tcp_port_number 1-65535>}	TCP ポート番号。TCP ポート番号は 1-65535 です。Web ベース管理ソフトウェアの一般的な TCP ポート番号は 80 です。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

HTTP を有効にし、ポート番号を設定します。

```
DES-3526:admin#enable web 80
Command: enable web 80

Success.

DES-3526:admin#
```

disable web

目的

スイッチの HTTP ベース管理ソフトウェアを無効にします。

構文

disable web

説明

スイッチの HTTP ベース管理ソフトウェアを無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

HTTP を無効にします。

```
DES-3526:admin#disable web
Command: disable web
Success.

DES-3526:admin#
```

save

目的

NV-RAM にスイッチ設定の変更を保存します。

構文

save

説明

NV-RAM に現在のスイッチ設定またはログファイルを入力します。保存されたスイッチ設定は、スイッチが再度起動するたびにスイッチのメモリにロードされます。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

NV-RAM に現在のスイッチ設定を入力します。

```
DES-3526:admin#save
Command: save

Saving all configurations to NV-RAM...Done.

DES-3526:admin#
```

reboot

目的

スイッチを再起動します。

構文

reboot

説明

スイッチを再起動します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチを再起動します。

```
DES-3526:admin#reboot
Command: reboot
Are you sure want to proceed with the system reboot? (y|n) y
Please wait, the switch is rebooting...
```

reboot force_agree

目的

スイッチを強制的に再起動します。

構文

reboot force_agree

説明

スイッチを強制的に再起動します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチを強制的に再起動します。

```
DES-3526:admin#reboot force_agree
Command: reboot force_agree
Please wait, the switch is rebooting...
```

reset

目的

スイッチを工場出荷時設定に戻します。

構文

reset {[config | system]}

説明

スイッチの設定を工場で割り当てられた初期設定に戻します。

パラメータ

パラメータ	説明
config	IP アドレス、ユーザアカウントおよびスイッチヒストリなどのパラメータが工場出荷時設定にリストアされます。スイッチは保存または再起動しません。
system	すべての工場出荷時設定がスイッチにリストアされます。スイッチは設定が初期値に変更された後、保存および再起動されます。再起動するとフォワーディングデータベース内のすべてのエントリがクリアされます。 パラメータを指定しないと、スイッチの現在の IP アドレス、ユーザアカウントおよびスイッチヒストリログは変更されません。他のすべてのパラメータは、工場出荷時設定にリストアされます。スイッチは保存または再起動しません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチのすべてのパラメータを初期値に戻します。

```
DES-3526:admin#reset config
Command: reset config

Are you sure to proceed with system reset?(y/n) y

Success.

DES-3526:admin#
```

login

目的

スイッチのコンソールにログインします。

構文

login

説明

ログインを開始します。ユーザ名とパスワードプロンプトが表示されます。

パラメータ

なし。

制限事項

なし。

使用例

ログインを開始します。

```
DES-3526:admin#login
Command: login

UserName:
```

logout

目的

スイッチコンソールからログアウトします。

構文

logout

説明

スイッチコンソールの現在のユーザセッションを終了します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチコンソールの現在のユーザセッションを終了します。

```
DES-3526:admin#logout
```

config command_prompt

目的

スイッチの CLI インタフェース用のコマンドプロンプトを設定します。

構文

config command_prompt [<string 16> | username | default]

説明

現在のコマンドプロンプトは「製品名」+「:」+「ユーザレベル」で構成されています。(例 : DES-3500: 5#) ユーザがスペースなしで半角英数字 16 文字を入力することによって「#」を除いたコマンドプロンプトのすべての部分と交換されます。または、ユーザがスイッチに設定した現在のログインユーザ名を入力することも可能です。

パラメータ

パラメータ	説明
<string 16>	16 文字までの半角英数字を入力し、CLI インタフェースにコマンドプロンプトを定義します。
username	現在の CLI コマンドプロンプトはスイッチに設定されたログインユーザ名に変更されます。
default	工場出荷時のコマンドプロンプトにリセットします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

コマンドプロンプトを「Tiberius」に変更します。

```
DES-3526:admin#config command_prompt Tiberius
Command: config command_prompt Tiberius

Success.

DES-3526:admin#
```

config greeting_message

目的

グリーティングメッセージまたはログインバナーを設定します。

構文

config greeting_message {default}

説明

グリーティングメッセージまたはログインバナーを設定します。

パラメータ

パラメータ	説明
default	工場出荷時のグリーティングメッセージにリセットします。 バナーエディタを開くためには、「config greeting_message」コマンドを使用します。情報を入力し、バナーエディタに記述されているコマンドを使用してバナーに表示します。 - 保存しないで終了 - Ctrl+C - 保存して終了 - Ctrl+W - カーソルの移動 - Left/Right/Up/Down - ラインの削除 - Ctrl+D - 全設定の消去 - Ctrl+X - オリジナルの設定のリロード - Ctrl+L

制限事項

管理者レベルおよびオペレータレベルユーザだけが本コマンドを実行できます。他の制限は以下の通りです。

- バナーは 6 行以内で指定します（1 行に 80 文字まで）。
- Ctrl+W は DRAM に変更されたバナーを保存するだけです。「save」コマンドを使用してフラッシュメモリに保存する必要があります。
- しきい値レベル内で有効です。

使用例

グリーティングメッセージを変更します。

```
DES-3526:admin#config greeting_message
Command: config greeting_message

Greeting Messages Editor
================================================================================

              DES-3526 Fast Ethernet Switch Command Line Interface

                             Firmware: Build 5.01-B19
          Copyright(C) 2000-2005 D-Link Corporation. All rights reserved.

================================================================================

   <Function Key>                    <Control Key>
   Ctrl+C     Quit without save      left/right/
   Ctrl+W     Save and quit            up/down     Move cursor
                                     Ctrl+D        Delete line
                                     Ctrl+X        Erase all setting
                                     Ctrl+L        Reload original setting
--------------------------------------------------------------------------------
```

show greeting_message

目的

スイッチに設定されている現在のグリーティングメッセージを参照します。

構文

show greeting_message

説明

スイッチに設定されている現在のグリーティングメッセージを参照します。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザだけが本コマンドを実行できます。

使用例

設定済みのグリーティングメッセージを参照します。

```
DES-3526:admin#show greeting_message
Command: show greeting_message

State : Enabled
================================================================================

               DES-3526 Fast Ethernet Switch Command Line Interface

                              Firmware: Build 5.01-B19
          Copyright(C) 2000-2005 D-Link Corporation. All rights reserved.

================================================================================


DES-3526:admin#
```

enable greeting_message

目的

スイッチに設定されている現在のグリーティングメッセージが表示されるようにします。

構文

enable greeting_message

説明

スイッチに設定されている現在のグリーティングメッセージが表示されるようにします。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに設定されている現在のグリーティングメッセージが表示されるようにします。

```
DES-3526:admin#enable greeting_message
Command: enable greeting_message
success
DES-3526:admin#
```

disable greeting_message

目的

スイッチに設定されている現在のグリーティングメッセージが表示されないようにします。

構文

disable greeting_message

説明

スイッチに設定されている現在のグリーティングメッセージが表示されないようにします。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに設定されている現在のグリーティングメッセージが表示されないようにします。

```
DES-3526:admin#disable greeting_message
Command: disable greeting_message
success
DES-3526:admin#
```

第 5 章　スイッチポートコマンド

コマンドラインインタフェース（CLI）におけるスイッチポートコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config ports	[<portlist | all>] {speed [auto | 10_half | 10_full |100_half | 100_full | 1000_full]} | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | trap [enable | disable] | description <desc 32>}
show ports	[<portlist>] {description} {err_disabled}

次のセクションから各コマンドについて詳しく記述します。

config ports

目的

スイッチのイーサネットポート設定を行います。

構文

config ports [<portlist | all>] {speed [auto | 10_half | 10_full |100_half | 100_full | 1000_full]} | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | trap [enable | disable] | description <desc 32>}

説明

スイッチのイーサネットポート設定を行います。<portlist> 内のあるポートだけに適用されます。

パラメータ

パラメータ	説明
<portlist>	• <portlist> - 設定するポートまたはポート範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - 全てのポートに設定します。
speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full]	指定ポートにポートスピードを設定します。 • auto - 指定したポート範囲にオートネゴシエーションを有効にします。 • 10_half - ポートスピードを 10M ハーフデュプレックスに設定します。 • 10_full - ポートスピードを 10M フルデュプレックスに設定します。 • 100_half - ポートスピードを 100M ハーフデュプレックスに設定します。 • 100_full - ポートスピードを 100M ハーフデュプレックスに設定します。 • 1000_full - ポートスピードを 1000M フルデュプレックスに設定します。 設定を行うと、ポートはデュプレックス、速度およびレイヤタイプに関連する能力を通知します。
flow_control [enable | disable]	指定ポートのフロー制御を「enable」（有効）または「disable」（無効）にします。
learning [enable | disable]	指定した範囲ポート上の MAC アドレス学習を「enable」（有効）または「disable」（無効）にします。
state [enable | disable]	指定ポート範囲を「enable」（有効）または「disable」（無効）にします。指定ポートがエラーによる無効状態である場合、本パラメータを有効にしてポートを有効状態に戻します。
trap [enable | disable]	スイッチのトラップ設定を「enable」（有効）または「disable」（無効）にします。
description <desc 32>	選択したポートインタフェースを説明するために 32 文字未満の半角英数字の文字列を入力します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチ 1 のポート 1-3 の速度を 10Mbps、フルデュプレックスに設定し、MAC アドレス学習と状態を有効にします。

```
DES-3526:admin#config ports all speed 10_full learning enable state enable
Command: config ports all speed 10_full learning enable state enable

Success.

DES-3526:admin#
```

show ports

目的

ポート範囲の現在の設定を表示します。

構文

show ports [<portlist>] {description} {err_disabled}

説明

ポート範囲の現在の設定を表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたはポート範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）
description	以前に入力したポート説明が表示されます。
err_disabled	無効ポートの接続状況と無効の理由を表示します。

制限事項

なし。

使用例

スイッチのすべてのポート設定を表示します。

```
DES-3526:admin#show ports
Command: show ports
Port  State/     Settings               Connection             Address  Trap
      MDIX       Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl  Learning State
----- ---------- ---------------------- ---------------------  -------- --------
1     Enabled    10M/Full/Disabled      Link Down              Enabled  Enabled
      Auto
2     Enabled    10M/Full/Disabled      Link Down              Enabled  Enabled
      Auto
3     Enabled    10M/Full/Disabled      Link Down              Enabled  Enabled
      Auto
4     Enabled    10M/Full/Disabled      Link Down              Enabled  Enabled
      Auto
5     Enabled    10M/Full/Disabled      Link Down              Enabled  Enabled
      Auto
6     Enabled    10M/Full/Disabled      Link Down              Enabled  Enabled
      Auto
7     Enabled    10M/Full/Disabled      Link Down              Enabled  Enabled
      Auto
8     Enabled    10M/Full/Disabled      Link Down              Enabled  Enabled
      Auto
9     Enabled    10M/Full/Disabled      Link Down              Enabled  Enabled
      Auto
10    Enabled    10M/Full/Disabled      Link Down              Enabled  Enabled
      Auto
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

第 6 章　ポートセキュリティコマンド

コマンドラインインタフェース（CLI）におけるポートセキュリティコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config port_security ports	[<portlist> | all] {admin_state [enable| disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}
delete port_security entry	vlan_name <vlan_name 32> mac_address <macaddr> port <port>
clear port_security_entry	port <portlist>
show port_security	{ports <portlist>}
enable port_security trap_log	
disable port_security trap_log	

次のセクションから各コマンドについて詳しく説明します。

config port_security ports

目的

ポートセキュリティを設定します。

構文

config port_security ports [<portlist> | all] {admin_state [enable| disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}

説明

ポートセキュリティ機能を設定します。<portlist> に示されたポートにだけ適用されます。

パラメータ

パラメータ	説明
<portlist> | all	• <portlist> - 設定するポートまたはポート範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - スイッチの全ポートに設定します。
admin_state [enable | disable]	リストアップされたポートへのセキュリティを「enable」（有効）または「disable」（無効）にします。
max_learning_addr <max_lock_no 0-64>	ポートへの FDB 内で動的に学習される MAC アドレス数を制限します。
lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]	アドレスをロックする手段を指定します。3 つの選択肢があります。 • Permanent - ロックされたアドレスは、エージングタイム経過後に削除されません。 • DeleteOnTimeout - ロックされたアドレスは、エージングタイム経過後に削除されます。 • DeleteOnReset - ロックされたアドレスは、リセットされるまで削除されません。

制限事項

管理者レベルまたはオペレータレベルユーザのみ本コマンドを実行できます。

使用例

ポートセキュリティを設定します。

```
DES-3526:admin#config port_security ports all admin_state enable max_learning_ad
dr 3 lock_address_mode Permanent
Command: config port_security ports all admin_state enable max_learning_addr 3 lock_
address_mode Permanent

Success.

DES-3526:admin#
```

delete port_security_entry

目的

MAC アドレス、ポート番号および VLAN ID ごとにポートセキュリティエントリを削除します。

構文

delete port_security_entry vlan_name <vlan_name 32> mac_address <macaddr> port <port>

説明

学習済みのポートセキュリティエントリを MAC アドレス、ポート番号および VLAN 名ごとに削除します。この機能は、ロックアドレスモードに「Permanent」か「DeleteOnReset」が選択されている場合にだけ適用されます。

パラメータ

パラメータ	説明
vlan_name <vlan_name 32>	削除するポートの対応する VLAN 名を入力します。
mac_address <macaddr>	削除するポートによって学習された MAC アドレスを入力します。
port <port>	入力済みの MAC アドレスを学習しているポート番号を入力します。ポートは、「:」(コロン)で分けることによって、最も下位のスイッチ番号と始めのポート番号によって指定されます。例えば、1:3 はスイッチ番号 1 のポート 3 を表しています。2:4 はスイッチ番号 2 のポート 4 を表しています。

制限事項

管理者レベルまたはオペレータレベルユーザのみ本コマンドを実行できます。

使用例

ポートセキュリティエントリを削除します。

```
DES-3526:admin#delete port_security_entry vlan_name default mac_address 00-01-30-10-2C-C7 port 1
Command: delete port_security_entry vlan_name default mac_address 00-01-30-10-2C-C7 port 1

ST_PortLock_DelSecEntry SUCCESS.

DES-3526:admin#
```

clear port_security_entry

目的

ポートセキュリティ機能のために指定ポートから学習した MAC アドレスエントリをクリアします。

構文

clear port_security_entry port <portlist>

説明

指定ポートごとにスイッチが学習した MAC アドレスエントリをクリアします。本コマンドはポートセキュリティ機能に関連するだけです。

パラメータ

パラメータ	説明
port <portlist>	設定するポートまたはポート範囲を指定します。ポートリストは、「:」(コロン) で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」(ダッシュ) を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」(カンマ)で分けます。(例 : 1:1-1:3,1:7-1:9)

制限事項

管理者レベルまたはオペレータレベルのみ本コマンドを実行できます。

使用例

ポートごとにポートセキュリティエントリをクリアします。

```
DES-3526:admin#clear port_security_entry port 1
Command: clear port_security_entry port 1

Success.

DES-3526:admin#
```

show port_security

目的

現在のポートセキュリティ設定を表示します。

構文

show port_security {ports <portlist>}

説明

このコマンドは、スイッチのポートに関するポートセキュリティ情報を表示するために使用されます。表示される情報には、ポートセキュリティ、Admin ステータス、学習しているアドレスの最大数およびロックモードが含まれます。

パラメータ

パラメータ	説明
<portlist>	参照するポートまたはポート範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

なし。

使用例

ポートセキュリティ設定を表示します。

```
DES-3526:admin#show port_security ports 1-5
Command: show port_security ports 1-5
Port_Security Trap/Log : Disabled
Port    Admin State  Max. Learning Addr.  Lock Address Mode
------  -----------  -------------------  -----------------
1       Enabled      3                    Permanent
2       Enabled      3                    Permanent
3       Enabled      3                    Permanent
4       Enabled      3                    Permanent
5       Enabled      3                    Permanent
```

enable port_security trap_log

目的

ポートセキュリティトラップログを表示します。

構文

enable port_security trap_log

説明

このコマンドは、スイッチのポートに関するポートセキュリティのトラップ情報を表示するために使用されます。

パラメータ

なし。

制限事項

なし。

使用例

ポートセキュリティのトラップログを表示します。

```
DES-3526:admin#enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-3526:admin#
```

disable port_security trap_log

目的

ポートセキュリティトラップログの表示を無効にします。

構文

disable port_security trap_log

説明

このコマンドは、スイッチのポートに関するポートセキュリティのトラップ情報の表示を無効にするために使用されます。

パラメータ

なし。

制限事項

なし。

使用例

ポートセキュリティのトラップログの表示を無効にします。

```
DES-3526:admin#disable port_security trap_log
Command: disable port_security trap_log

Success.

DES-3526:admin#
```

第 7 章　ネットワーク管理（SNMP）コマンド

本スイッチシリーズは、SNMP（Simple Network Management Protocol）バージョン 1、2c および 3 をサポートしています。スイッチのモニタおよび制御のためには、SNMP を有効にした後に、SNMP のバージョンを指定します。SNMP の 3 つのバージョンは、管理ステーションとネットワークデバイス間に提供するセキュリティレベルが異なります。3 つの SNMP バージョンのセキュリティ機能は以下の通りです。

SNMP バージョン	認証方式	説明
v1	コミュニティ名	NoAuthNoPriv - コミュニティ名が認証に使用されます。
v2c	コミュニティ名	NoAuthNoPriv - コミュニティ名が認証に使用されます。
v3	ユーザ名	NoAuthNoPriv - ユーザ名が認証に使用されます。
v3	MD5 または SHA	AuthNoPriv - 認証は HMAC-MD5 または HMAC-SHA アルゴリズムに基づきます。
v3	MD5 DES または SHA DES	AuthPrivDES - 認証は HMAC-MD5 または HMAC-SHA アルゴリズムに基づきます。 56 ビット暗号方式が CBC-DES（DES-56）標準規格に基づいて追加されます。

コマンドラインインタフェース（CLI）におけるネットワーク管理コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create snmp user	<snmp_username 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16 > | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}
delete snmp user	<snmp_username 32>
show snmp user	
create snmp view	<view_name 32> <oid> view_type [included | excluded]
delete snmp view	<view_name 32> [all | oid]
show snmp view	<view_name 32>
create snmp community	<community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community	<community_string 32>
show snmp community	<community_string 32>
config snmp engineID	<snmp_engineID>
show snmp engineID	
create snmp group	<groupname 32> {v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]} {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}
delete snmp group	<groupname 32>
show snmp groups	
create snmp host	<ipaddr> {v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]}　<auth_string 32>
delete snmp host	<ipaddr>
show snmp host	<ipaddr>
create trusted_host	<ipaddr>| network<network_address>
delete trusted_host	[all | ipaddr<ipaddr>| network<network_address>]
show trusted_host	
enable snmp traps	
enable snmp authenticate traps	
show snmp traps	
disable snmp traps	
disable snmp authenticate traps	
config snmp system_contact	<sw_contact>
config snmp system_location	<sw_location>
config snmp system_name	<sw_name>
enable rmon	
disable rmon	

次のセクションから各コマンドについて詳しく説明します。

create snmp user

目的

新しい SNMP ユーザを作成し、本コマンドで作成した SNMP グループにユーザを追加します。

構文

create snmp user <snmp_username 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}

説明

新しい SNMP ユーザを作成し、本コマンドで作成した SNMP グループにユーザを追加します。SNMP は以下の項目を保証します。

- メッセージの保全 - パケットが送信中に変更されていないことを保証します。
- 認証 - SNMP メッセージが有効な送信元から来ているかどうかを判断します。
- 暗号化 - 未認証の送信元によって参照されることを防ぐために、メッセージの内容にスクランブルをかけます。

パラメータ

パラメータ	説明
<snmp_username 32>	新しい SNMP ユーザを識別する名前。（半角英数字 32 文字以内。）
<groupname 32>	新しい SNMP ユーザが対応付けされる SNMP グループを識別する名前。（半角英数字 32 文字以内。）
encrypted	SNMP を使用した認証のタイプを選択します。 • by_password - 認証とプライバシーのために SNMP ユーザにパスワードを入力するように要求します。パスワードは、以下で「auth_password」を指定することによって定義されます。この方式を推奨します。 • by_key - 認証とプライバシーのために SNMP ユーザに暗号化キーを入力するように要求します。キーは、以下のフィールドにおいて 16 進数形式で指定することによって定義されます。この方式は推奨されません。
auth	SNMP ユーザを認証するために使用される認証アルゴリズムのタイプを選択します。 • md5 - HMAC-MD5-96 認証レベルを使用します。md5 は、以下のタイプから 1 つを選択し、入力することによって利用されます。 - <auth password 8-16> - ホストに対するパケットを受信するためにエージェントを認可するために使用されるパスワードです。半角英数字 8-16 文字。 - <auth_key 32-32> - ホストに対するパケットを受信するためにエージェントを認可するために使用されるキーです。16 進数形式 32 文字。 • sha - HMAC-SHA-96 認証レベルを使用します。 - <auth password 8-20> - ホストに対するパケットを受信するためにエージェントを認可するために使用されるパスワードです。半角英数字 8-20 文字。 - <auth_key 40-40> - ホストに対するパケットを受信するためにエージェントを認可するために使用されるキーです。16 進数形式 40 文字。 • priv - priv（プライバシー）パラメータを追加すると、より高いセキュリティために認証アルゴリズムに加えて、暗号化も可能になります。 - des - 本パラメータを追加すると、56 ビットの暗号化のための DES-56 標準の使用が可能となります。 · <priv_password 8-16> - ホストがエージェントに送信するメッセージの内容を暗号化するために使用されます。半角英数字 8-16 文字の文字列。 · <priv_key 32-32> - ホストがエージェントに送信するメッセージの内容を暗号化するために使用されます。16 進数形式 32 文字。 - none - 本パラメータを追加すると、暗号化を行いません。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチに SNMP ユーザを作成します。

```
DES-3526:admin#create snmp user dlink default encrypted by_password auth md5 canadian priv none
Command: create snmp user dlink default encrypted by_password auth md5 canadian priv none

Success.

DES-3526:admin#
```

delete snmp user

目的

SNMP ユーザテーブルから SNMP ユーザを削除します。

構文

delete snmp user <snmp_username 32>

説明

SNMP グループから SNMP ユーザテーブルを削除します。

パラメータ

パラメータ	説明
<snmp_username 32>	削除する SNMP ユーザを特定する文字列（半角英数字 32 文字以内）。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチに設定済みの SNMP ユーザを削除します。

```
DES-3526:admin#delete snmp user dlink
Command: delete snmp user dlink

Success.

DES-3526:admin#
```

show snmp user

目的

SNMP ユーザテーブルの各 SNMP ユーザ名に関する情報を表示します。

構文

show snmp user

説明

SNMP ユーザテーブルの各 SNMP ユーザ名に関する情報を表示します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチに現在設定されている SNMP ユーザを表示します。

```
DES-3526:admin#show snmp user
Command: show snmp user

Username         Group Name       SNMP Version  Auth-Protocol  PrivProtocol
---------------  ---------------  ------------  -------------  ------------
initial          initial          V3            None           None

Total Entries : 1

DES-3526:admin#
```

create snmp view

目的

MIB オブジェクトと SNMP マネージャのアクセスを制限するために、コミュニティ名にビューを割り当てます。

構文

create snmp view <view_name 32> <oid> view_type [included | excluded]

説明

SNMP マネージャがアクセス可能な MIB オブジェクトを制限するために、コミュニティ名にビューを割り当てます。

パラメータ

パラメータ	説明
<view_name 32>	32 文字までの半角英数字を入力します。新しい SNMP ビューを登録し、識別する際に使用します。
<oid>	SNMP マネージャがアクセス可能な範囲であるかを指定するオブジェクトツリー（MIB ツリー）を識別するオブジェクト ID。
view type [included |excluded]	以下のビュータイプを選択します。 • included - SNMP マネージャがアクセスできるオブジェクトのリストにこのオブジェクトを含めます。 • excluded - SNMP マネージャがアクセスできるオブジェクトのリストからこのオブジェクトを除外します。

使用例

SNMP ビューを作成します。

```
DES-3526:admin#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DES-3526:admin#
```

delete snmp view

目的

スイッチに作成済みの SNMP ビューエントリを削除します。

構文

delete snmp view <view_name 32> [all | <oid>]

説明

スイッチに作成 SNMP ビューエントリを削除します。

パラメータ

パラメータ	説明
<view_name 32>	削除する SNMP ビュー名（32 文字以内の半角英数字）。
all | <oid>	• all - スイッチの SNMP ビューすべてを削除します。 • oid - スイッチから削除されるオブジェクトツリー（MIB ツリー）を示すオブジェクト ID を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチから設定した SNMP ビューを削除します。

```
DES-3526:admin#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DES-3526:admin#
```

show snmp view

目的

スイッチに作成済みの SNMP ビューを表示します。

構文

show snmp view {<view_name 32>}

説明

スイッチに作成済みの SNMP ビューを表示します。

パラメータ

パラメータ	説明
<view_name 32>	削除する SNMP ビュー名が表示されます（32 文字以内の半角英数字）。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP ビュー設定を表示します。

```
DES-3526:admin#show snmp view
Command: show snmp view

Vacm View Table Settings

View Name : restricted
Subtree   : 1.3.6.1.2.1.1
View Type : Included
View Mask :

View Name : restricted
Subtree   : 1.3.6.1.2.1.11
View Type : Included
View Mask :

View Name : restricted
Subtree   : 1.3.6.1.6.3.10.2.1
View Type : Included
View Mask :

View Name : restricted
Subtree   : 1.3.6.1.6.3.11.2.1
View Type : Included
View Mask :

View Name : restricted
Subtree   : 1.3.6.1.6.3.15.1.1
View Type : Included
View Mask :

View Name : CommunityView
Subtree   : 1
View Type : Included
View Mask :

View Name : CommunityView
Subtree   : 1.3.6.1.6.3
View Type : Excluded
View Mask :

View Name : CommunityView
Subtree   : 1.3.6.1.6.3.1
View Type : Included
View Mask :


Total Entries : 8

DES-3526:admin#
```

create snmp community

目的

SNMP マネージャとエージェントとの関係を定義するために SNMP コミュニティ名を作成します。コミュニティ名は、スイッチ上のエージェントへのアクセスを行う際のパスワードの役割をします。以下の特性はコミュニティ名と関係します。

- アクセスリストはコミュニティ名を使用して、スイッチ上の SNMP エージェントにアクセスを行う SNMP マネージャの IP アドレスが掲載されています。
- MIB ビューは SNMP コミュニティにアクセス可能なすべての MIB オブジェクトのサブセットを定義します。
- SNMP コミュニティにアクセス可能な MIB オブジェクトには「read_write」（読み書き可能）または「read_only」（読み出しのみ可能）のレベルがあります。

構文

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]

説明

SNMP コミュニティ名を作成し、このコミュニティ名にアクセス制限を行う文字列を割り当てます。

パラメータ

パラメータ	説明
<community_string 32>	スイッチの SNMP コミュニティのメンバを識別します（32 文字までの半角英数字）。本コミュニティ名は、リモートの SNMP マネージャが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。
view <view_name 32>	リモート SNMP マネージャがスイッチにアクセスできる MIB オブジェクトのグループを指定します（32 文字までの半角英数字）。
[read_only | read_write]	以下のビュータイプを選択します。 • read_only - 本コマンドを使用して作成したコミュニティ名を使用する SNMP コミュニティメンバは、スイッチの MIB オブジェクトの内容を読み出しが可能です。 • read_write - 本コマンドを使用して作成したコミュニティ名を使用する SNMP コミュニティメンバは、スイッチの MIB オブジェクトの内容を読み出しおよび書き込みが可能です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP コミュニティ名「dlink」を作成します。

```
DES-3526:admin#create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.

DES-3526:admin#
```

delete snmp community

目的

スイッチから特定の SNMP コミュニティ名を削除します。

構文

delete snmp community <community_string 32>

説明

スイッチから定義済みの SNMP コミュニティ名を削除します。

パラメータ

パラメータ	説明
<community_string 32>	スイッチの SNMP コミュニティのメンバを識別します（32 文字までの半角英数字）。本コミュニティ名は、リモートの SNMP マネージャが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP コミュニティ名「dlink」を削除します。

```
DES-3526:admin#delete snmp community dlink
Command: delete snmp community dlink

Success.

DES-3526:admin#
```

show snmp community

目的

スイッチの設定されている SNMP コミュニティ名を表示します。

構文

show snmp community {<community_string 32>}

説明

スイッチに設定されている SNMP コミュニティ名を表示します。

パラメータ

パラメータ	説明
<community_string 32>	スイッチの SNMP コミュニティのメンバを識別します（32 文字までの半角英数字）。本コミュニティ名は、リモートの SNMP マネージャが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

現在入力されている SNMP コミュニティ名を表示します。

```
DES-3526:admin#show snmp community
Command: show snmp community

SNMP Community Table
Index : private
Community Name                  View Name                       Access Right
------------------------------  ------------------------------  ------------
private                         CommunityView                   read_write
Index : public
Community Name                  View Name                       Access Right
------------------------------  ------------------------------  ------------
public                          CommunityView                   read_only

Total Entries : 2

DES-3526:admin#
```

config snmp engineID

目的

スイッチの SNMP エンジンに識別子を設定します。

構文

config snmp engineID <snmp_engineID >

説明

スイッチの SNMP エンジンに識別子を設定します。

パラメータ

パラメータ	説明
<snmp_engineID >	スイッチの SNMP エンジンを指定します。（10-64 文字の 16 進数 0-9、A-F）

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

「0035636666」という名前をスイッチの SNMP エージェントに付与します。

```
DES-3526:admin#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

DES-3526:admin#
```

show snmp engineID

目的

スイッチの SNMP エンジンの識別子を表示します。

構文

show snmp engineID

説明

スイッチの SNMP エンジンの識別子を表示します。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチの SNMP エンジンの現在の名前を表示します。

```
DES-3526:admin#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DES-3526:admin#
```

create snmp group

目的

新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを作成します。

構文

create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}

説明

新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを作成します。

パラメータ

パラメータ	説明
<groupname 32>	新しい SNMP ユーザに割り当てる SNMP グループを指定します。（32 文字までの半角英数字）
[v1 | v2c | v3]	• v1 - SNMP バージョン 1 が使用されます。Simple Network Management Protocol（SNMP）バージョン 1 は、モニタする手段と制御ネットワークデバイスを提供するネットワーク管理プロトコルです。 • v2c - SNMP バージョン 2c が使用されます。SNMP v2c は、ネットワークマネジメント管理を中央に集結して、提供します。SNMP バージョン 1 と比較して SMI（Structure of Management Information）およびセキュリティ機能において強化されています。 • v3 - SNMP バージョン 3 が使用されます。SNMP v3 は、ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。SNMP v3 では以下のパラメータを追加します。 - メッセージの保全 - パケットが送信中に変更されていないことを保証します。 - 認証 - SNMP メッセージが有効な送信元から来ているかどうかを判断します。 - 暗号化 - 未認証の送信元に参照されることを防ぐために、メッセージの内容にスクランブルをかけます。
[noauth_nopriv | auth_nopriv | auth_priv]noauth_nopriv]	• noauth_nopriv - スイッチとリモート SNMP マネージャ間に送信されるパケットには許可も暗号化もありません。 • auth_nopriv - スイッチとリモート SNMP マネージャ間には認証は必要ですが、送信パケットには暗号化はありません。 • auth_priv - スイッチとリモート SNMP マネージャ間には認証と送信パケットの暗号化が必要です。
read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>	• read_view - 作成された SNMP グループが、SNMP メッセージを要求するように指定します。 • write_view - 作成された SNMP グループが、書き込み権を持つように指定します。 • notify_view - 作成された SNMP グループが、スイッチの SNMP エージェントによって生成された SNMP トラップメッセージを受信するように指定します。 <view_name 32> - リモート SNMP マネージャがスイッチにアクセスできる MIB オブジェクトのグループを指定します。（32 文字までの半角英数字）

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP グループ名「sg1」を作成します。

```
DES-3526:admin#create snmp group sg1 v3 noauth_nopriv read_view v1 write_view v1 notify_view v1
Command: create snmp group sg1 v3 noauth_nopriv read_view v1 write_view v1 notify_view v1

Success.

DES-3526:admin#
```

delete snmp group

目的

スイッチから SNMP グループを削除します。

構文

delete snmp group <groupname 32>

説明

スイッチから SNMP グループを削除します。

パラメータ

パラメータ	説明
<groupname 32>	新しい SNMP ユーザが割り当てられる SNMP グループを特定する 32 文字以内の半角英数字名。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

「sg1」という名前の SNMP グループを削除します。

```
DES-3526:admin#delete snmp group sg1
Command: delete snmp group sg1

Success.

DES-3526:admin#
```

show snmp groups

目的

スイッチに現在設定されている SNMP グループのグループ名を表示します。また、各グループのセキュリティモデル / レベルおよびステータスを表示します。

構文

show snmp groups

説明

現在のスイッチに設定した SNMP グループ名を表示します。また、各グループのセキュリティモデル / レベルおよびステータスを表示します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチの現在設定されている SNMP グループを表示します。

```
DES-3526:admin#show snmp groups
Command: show snmp groups
Vacm Access Table Settings

Group    Name    : Group3
ReadView Name    : ReadView
WriteView Name   : WriteView
Notify View Name : NotifyView
Security Model   : SNMPv3
Security Level   : NoAuthNoPriv

Group    Name    : initial
ReadView Name    : restricted
WriteView Name   :
Notify View Name : restricted
Security Model   : SNMPv3
Security Level   : NoAuthNoPriv

Group    Name    : ReadGroup
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : ReadGroup
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Security Model   : SNMPv2
Security Level   : NoAuthNoPriv

Group    Name    : WriteGroup
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : WriteGroup
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv2
Security Level   : NoAuthNoPriv

Total Entries : 6

DES-3526:admin#
```

create snmp host

目的

スイッチの SNMP エージェントによって生成される SNMP トラップの受信者を作成します。

構文

create snmp host <ipaddr> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv] <auth_string 32>]

説明

スイッチの SNMP エージェントによって生成される SNMP トラップの受信者を作成します。

パラメータ

パラメータ	説明
host <ipaddr>	• host <ipaddr> - スイッチの SNMP ホストとして動作するリモート管理ステーションの IPv4 アドレス。
v1 | v2c | v3	• v1 - SNMP バージョン 1 を使用します。Simple Network Management Protocol（SNMP）バージョン 1 は、モニタする手段と制御ネットワークデバイスを提供するネットワーク管理プロトコルです。 • v2c - SNMP バージョン 2c を使用します。SNMP v2c は、ネットワークマネジメント管理を中央に集結して、提供します。SNMP バージョン 1 と比較して SMI（Structure of Management Information）およびセキュリティ機能において強化されています。 • v3 - SNMP バージョン 3 が使用されます。SNMP v3 は、ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。SNMP v3 では以下のパラメータを追加します。 - メッセージの保全 - パケットが送信中に変更されていないことを保証します。 - 認証 - SNMP メッセージが有効な送信元から来ているかどうかを判断します。 - 暗号化 - 未認証の送信元によって参照されることを防ぐために、メッセージの内容にスクランブルをかけます。
noauth_nopriv | auth_nopriv | auth_priv	• noauth_nopriv - スイッチとリモート SNMP マネージャ間に送信されるパケットには許可も暗号化もありません。 • auth_nopriv - スイッチとリモート SNMP マネージャ間には認証は必要ですが、送信パケットには暗号化はありません。 • auth_priv - スイッチとリモート SNMP マネージャ間には認証と送信パケットの暗号化が必要です。
<auth_sting 32>	スイッチの SNMP エージェントがスイッチにアクセスするためにリモートの SNMP マネージャを認可するために使用する文字列。（32 文字までの半角英数字。）

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SNMP メッセージを受信するために SNMP IPv4 ホストを作成します。

```
DES-3526:admin#create snmp host 10.48.74.100 v3 auth_priv public
Command: create snmp host 10.48.74.100 v3 auth_priv public

Success.

DES-3526:admin#
```

delete snmp host

目的

スイッチの SNMP エージェントによって生成された SNMP トラップの受信者を削除します。

構文

delete snmp [host <ipaddr>]

説明

スイッチの SNMP エージェントによって生成された SNMP トラップの受信者を削除します。

パラメータ

パラメータ	説明
host<ipaddr>	スイッチの SNMP ホストとして動作するリモート管理ステーションの IPv4 アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IPv4 SNMP ホストエントリを削除します。

```
DES-3526:admin#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DES-3526:admin#
```

show snmp host

目的

スイッチの SNMP エージェントによって生成される SNMP トラップの受信者を表示します。

構文

show snmp host {<ipaddr>}

説明

スイッチの SNMP エージェントによって生成される SNMP トラップの受信者として選出されたリモート SNMP マネージャの IP アドレスおよび設定情報を表示します。

パラメータ

パラメータ	説明
<ipaddr>	スイッチの SNMP エージェントによって生成された SNMP トラップを受け取るリモート SNMP マネージャの IP アドレス。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチに現在設定されている SNMP ホストを表示します。

```
DES-3526:admin#show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version  Community Name/SNMPv3 User Name
---------------  ------------  ------------------------------
10.48.76.23      V2c           private
10.48.74.100     V3            authpriv public

Total Entries:2

DES-3526:admin#
```

create trusted_host

目的

トラストホストを作成します。

構文

create trusted_host [<ipaddr> | network <network_address>] {snmp | telnet | ssh | http | https}

説明

トラストホストを作成します。4 個までの IP アドレスが SNMP または Telnet ベースの管理ソフトウェア経由でスイッチを管理することができます。これらの IP アドレスは、マネジメント VLAN に所属する必要があります。IP アドレスが指定されない場合、ユーザがユーザ名およびパスワードを知っていても、どの IP アドレスからもスイッチへのアクセスはできません。

パラメータ

パラメータ	説明
<ipaddr>	指定した IP アドレスのトラストホストを作成します。
network <network_address>	指定したネットワークアドレスのトラストホストを作成します。
{snmp | telnet | ssh | http | https}	作成するトラストホストのプロトコルを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

トラストホストを作成します。

```
DES-3526:admin#create trusted_host 1.11.11.11
Command: create trusted_host 1.11.11.11

Success.

DES-3526:admin#
```

delete trusted_host

目的

上記「create trusted_host」コマンドで作成したトラストホストエントリを削除します。

構文

delete trusted host ipaddr [ipaddr <ipaddr> | network <network_address> | all]

説明

上記「create trusted_host」コマンドで作成したトラストホストエントリを削除します。

パラメータ

パラメータ	説明
ipaddr <ipaddr>	削除するトラストホストの IP アドレス。
network <network_address>	削除するトラストホストのネットワークアドレス。
all	すべてのトラストホストを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IP アドレス「10.48.74.121」を持つトラストホストを削除します。

```
DES-3526:admin#delete trusted_host 1.11.11.11
Command: delete trusted_host 1.11.11.11

Success.

DES-3526:admin#
```

show trusted_host

目的

「create trusted_host」コマンドでスイッチに作成したトラストホストのリストを表示します。

構文

show trusted_host <ipaddr>

説明

上記「create trusted_host」コマンドでスイッチに作成したトラストホストのリストを表示します。

パラメータ

パラメータ	説明
<ipaddr>	参照するトラストホストの IP アドレス。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

トラストホストのリストを表示します。

```
DES-3526:admin#show trusted_host
Command: show trusted_host

Management Stations

IP Address
-----------
10.53.13.94

Total Entries:1

DES-3526:admin#
```

enable snmp traps

目的

SNMP トラップサポートを有効にします。

構文

enable snmp traps

説明

スイッチの SNMP トラップサポートを有効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチの SNMP トラップサポートを有効にします。

```
DES-3526:admin#enable snmp traps
Command: enable snmp traps

Success.

DES-3526:admin#
```

enable snmp authenticate traps

構文

enable snmp authenticate_traps

説明

スイッチの SNMP 認証トラップサポートを有効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

SNMP 認証トラップサポートを有効にします。

```
DES-3526:admin#enable snmp authenticate traps
Command: enable snmp authenticate traps

Success.

DES-3526:admin#
```

show snmp traps

目的

スイッチの SNMP トラップサポートを表示します。

構文

show snmp traps

説明

スイッチの SNMP トラップサポートを表示します。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

現在の SNMP トラップサポートを参照します。

```
DES-3526:admin#show snmp traps
Command: show snmp traps
SNMP Trap          : Enabled
Authenticate Traps : Enabled
DES-3526:admin#
```

disable snmp traps

目的

スイッチの SNMP トラップサポートを無効にします。

構文

disable snmp traps

説明

スイッチの SNMP トラップサポートを無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチの SNMP トラップサポートを無効にします。

```
DES-3526:admin#disable snmp traps
Command: disable snmp traps

Success.

DES-3526:admin#
```

disable snmp authenticate traps

目的

SNMP 認証トラップサポートを無効にします。

構文

disable snmp authenticate traps

説明

スイッチの SNMP 認証トラップサポートを無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

SNMP 認証トラップサポートを無効にします。

```
DES-3526:admin#disable snmp authenticate traps
Command: disable snmp authenticate traps

Success.

DES-3526:admin#
```

config snmp system_contact

目的

スイッチを管理するコンタクトパーソン名を入力します。

構文

config snmp system_contact <sw_contact>

説明

スイッチを管理するコンタクトパーソンを識別する名前および（または）情報（半角英数字 255 文字以内）を入力します。

パラメータ

パラメータ	説明
<sw_contact>	255 文字までを使用できます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチのコンタクトパーソンに「netadmin」を設定します。

```
DES-3526:admin#config snmp system_contact netadmin
Command: config snmp system_contact netadmin

Success.

DES-3526:admin#
```

config snmp system_location

目的

スイッチの設置場所の説明を入力します。

構文

config snmp system_location <sw_location>

説明

スイッチの設置場所の説明を入力するために使用されます。

パラメータ

パラメータ	説明
<sw_location>	半角英数字 255 文字までを使用できます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチ設置場所に「lab a」を設定します。

```
DES-3526:admin#config snmp system_location lab a
Command: config snmp system_location lab a

Success.

DES-3526:admin#
```

config snmp system_name

目的

スイッチに名前を設定します。

構文

config snmp system_name <sw_name>

説明

スイッチに名前を設定します。

パラメータ

パラメータ	説明
<sw_name>	255 文字まで使用できます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチ名に「DES-3500 」を設定します。

```
DES-3526:admin#config snmp system_name DES-3500
Command: config snmp system_name DES-3500

Success.

DES-3526:admin#
```

enable rmon

目的

スイッチの RMON 機能を有効にします。

構文

enable rmon

説明

スイッチでリモートモニタリング機能（RMON）を有効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

RMON を有効にします。

```
DES-3526:admin#enable rmon
Command: enable rmon

Success.

DES-3526:admin#
```

disable rmon

目的

スイッチの RMON 機能を無効にします。

構文

disable rmon

説明

スイッチのリモートモニタリング機能（RMON）を無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

RMON を無効にします。

```
DES-3526:admin#disable rmon
Command: disable rmon

Success.

DES-3526:admin#
```

第 8 章　スイッチユーティリティコマンド（ファイルシステムコマンドを含む）

コマンドラインインタフェース（CLI）におけるスイッチユーティリティコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
download	[firmware_fromTFTP <ipaddr> <path_filename 64> {image_id <int 1-2>} | cfg_fromTFTP <ipaddr> <path_filename 64> {increment}]
config firmware	image_id <int 1-2> [delete | boot_up]
show firmware_information	
show config	[current_config | config_in_nvram]
upload	[cfg_toTFTP | log_toTFTP] <ipaddr> <path_filename 64>
enable autoconfig	
disable autoconfig	
show autoconfig	
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}

次のセクションから各コマンドについて詳しく説明します。

download

目的

TFTP サーバから新しいファームウェアまたはスイッチのコンフィグレーションファイルをダウンロードしてインストールします。

構文

download [firmware_fromTFTP <ipaddr> <path_filename 64> {image_id <int 1-2>} | cfg_fromTFTP <ipaddr> <path_filename 64> {increment}]

説明

TFTP サーバから新しいファームウェアまたはスイッチのコンフィグレーションファイルをダウンロードします。既に割り当てている「c:\drive」を使用して、スイッチのフラッシュメモリにあるファームウェアまたはコンフィグレーションファイルを保存します。

パラメータ

パラメータ	説明
firmware_fromTFTP	新しいファームウェアを TFTP サーバからスイッチにダウンロードしてインストールします。 • <ipaddr> - TFTP サーバの IPv4 アドレス。 • <path_filename 64> - TFTP サーバ上のファームウェアファイルの DOS パスとファイル名。例 : c: \DES3500.had • image_id <int 1-2> - <int 1-2> - スイッチメモリにおけるファームウェアのイメージ番号を指定します。スイッチのメモリには 2 個のファームウェアイメージを格納できます。変更されない限り、ID1 が初期設定の起動用ファームウェアです。
cfg_fromTFTP	新しいコンフィグレーションファイルを TFTP サーバからスイッチにダウンロードしてインストールします。 • <ipaddr> - TFTP サーバの IPv4 アドレス。 • <path_filename 64> - TFTP サーバ上のコンフィグレーションの DOS パスとファイル名。例 : c: \des3500.had • increment - 部分的なスイッチコンフィグレーションファイルのダウンロードが可能です。コンフィグレーションファイル内に明記されているスイッチパラメータだけを変更するようにファイルをダウンロードすることができます。他のすべてのスイッチパラメータは変更されないで残ります。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

コンフィグレーションファイルをダウンロードします。

```
DES-3526:admin#download cfg_fromTFTP 10.48.74.121 unit all c:\cfg\setting.txt
Command: download cfg_fromTFTP 10.48.74.121 unit all c:\cfg\setting.txt

Connecting to server...................Done.
Download configuration.................Done.

DES-3526:admin#
DES-3526:admin##-------------------------------------------------------------
DES-3526:admin##                  DES-3526 Configuration
DES-3526:admin##
DES-3526:admin##                  Firmware:Build 5.01-B19
DES-3526:admin## Copyright(C) 2008 D-Link Corporation.All rights reserved.
DES-3526:admin##-------------------------------------------------------------
DES-3526:admin#
DES-3526:admin## BASIC
DES-3526:admin#
DES-3526:admin#config serial_port baud_rate 9600 auto_logout 10_minutes
Command: config serial_port baud_rate 9600 auto_logout 10_minutes
DES-3526:admin#disable authen_policy
Command: disable authen_policy

Success.

DES-3526:admin#
DES-3526:admin##-------------------------------------------------------------
DES-3526:admin##              End of configuration file for DES-3526
DES-3526:admin##-------------------------------------------------------------
DES-3526:admin#
```

「download cfg_fromTFTP」コマンドは、コンフィグレーションファイル内にリストアップされている順に各種設定のローディングを始めます。ファイルがロードに成功すると、「End of configuration file for DES-3526」というメッセージがコマンドプロンプトに表示されます。

スイッチのフラッシュメモリにファームウェアファイルをダウンロードします。

```
DES-3526:admin#download firmware_fromTFTP 10.53.13.201 c:\3500firm.had c:\ firm1
Command: download firmware_fromTFTP 10.53.13.201 c:\3500firm.had c:\ firm1

Connecting to server.........Done.
Download firmware............Done.  Do not power off!
Upload file to FLASH.........Done.

DES-3526:admin#
```

upload

目的

スイッチの設定またはスイッチのヒストリログを TFTP サーバにアップロードします。

構文

upload [cfg_toTFTP | log_toTFTP] <ipaddr> <path_filename 64>

説明

TFTP サーバにコンフィグレーションファイルまたはログファイルをアップロードします。既に割り当てている「c:\drive」を使用して、スイッチのフラッシュメモリにあるログファイルまたはコンフィグレーションファイルを保存します。

パラメータ

パラメータ	説明
cfg_toTFTP	現在のスイッチのコンフィグレーションファイルまたはスイッチのフラッシュメモリに保存されているコンフィグレーションファイルを TFTP サーバにアップロードします。 • <ipaddr> - TFTP サーバの IPv4 アドレス。 • <path_filename 64> - TFTP サーバにアップロードするログファイルの DOS パスとファイル名。（例 : c: \3500.txt）
log_toTFTP	現在のスイッチのログファイルまたはスイッチのフラッシュメモリに保存されているログファイルを TFTP サーバにアップロードします。 • <ipaddr> - TFTP サーバの IPv4 アドレス。 • <path_filename 64> - TFTP サーバにアップロードするログファイルの DOS パスとファイル名。（例 c:\3500.txt）

制限事項

管理者レベルまたはオペレータレベルユーザのみ本コマンドを実行できます。

使用例

コンフィグレーションファイルをアップロードします。

```
DES-3526:admin#upload cfg_toTFTP 10.53.13.3 c:\3500.cfg
Command: upload cfg_toTFTP 10.53.13.3 c:\3500.cfg

Connecting to server............Done.
Upload configuration............Done.

DES-3526:admin#
```

スイッチのフラッシュメモリにコンフィグレーションファイルをアップロードします。

```
DES-3526:admin#upload cfg_toTFTP 10.53.13.3 c:\3500.cfg c:\ startup.cfg
Command: upload cfg_toTFTP 10.53.13.3 c:\3500.cfg c:\ startup.cfg

Connecting to server............Done.
Upload configuration............Done.

DES-3526:admin#
```

config firmware image_id

目的

起動用セクションとしてフラッシュメモリ内のファームウェアファイルを設定します。

構文

config firmware image_id <int 1-2> [delete | boot_up]

説明

起動用セクションとしてスイッチのフラッシュメモリ内のファームウェアファイルを設定します。

パラメータ

パラメータ	説明
<int_id 1-12>	ファームウェアイメージを設定するスイッチスタック内のスイッチの ID を指定します。
delete	本パラメータを入力し、特定のファームウェアセクションを削除します。
boot_up	本パラメータを入力し、起動セクションとしてファームウェアイメージ ID を指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

起動セクションとしてファームウェアセクション 1 を設定します。

```
DES-3526:admin#config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

DES-3526:admin#
```

show config

目的

スイッチのコンフィグレーション設定の現在または保存されているバージョンを表示します。

構文

show config [current_config | config_in_nvram]

説明

NV RAM に保存されているすべてのコンフィグレーション設定を表示します。または、現在設定されているコンフィグレーション設定を表示します。キーボードを使用して、一度に 1 行ずつ（Enter キー）、一度に 1 ページずつ（スペースキー）、またはすべて（a キー）を表示することができます。コンフィグレーション設定は以下の順にカテゴリごとにリスト表示されます。

1. BASIC	18. MAC_ADDRESS_TABLE_NOTIFICATION
2. STORM	19. STP
3. LOOP_DETECT	20. SSH
4. GM	21. SSL
5. GM_H [H]	22. SAFE_GUARD
6. SYSLOG	23. ACL
7. QOS	24. SNTP
8. MIRROR	25. IPBIND
9. TRAF-SEGMENTATION	26. DHCP_NETBIOS_FILTER
10. PORT	27. ROUTE
11. PORT_LOCK	28. SNOOP
12. 8021X	29. LACP
13. SNMPv3	30. GVLAN
14. SNMPv3User [H]	31. IP
15. MANAGEMENT	32. ARP
16. VLAN	33. ACCESS_AUTHENTICATION_CONTROL
17. FDB	34. DHCP_RELAY

パラメータ

パラメータ	説明
current_config	本パラメータを入力すると、NVRAM に保存せずに入力したコンフィグレーションを表示します。
config_in_nvram	本パラメータを入力すると、NVRAM に保存してあるコンフィグレーションを表示します。

制限事項

なし。

使用例

現在のコンフィグレーション設定を参照します。

```
DES-3526:admin#show config current_config
Command: show config current_config
#-----------------------------------------------------------------
# DES-3526 Configuration
#
# Firmware: Build 4.01-B19
# Copyright(C) 2000-2004 D-Link Corporation. All rights reserved.
#-----------------------------------------------------------------
# BASIC
config serial_port baud_rate 9600 auto_logout 10_minutes
enable telnet 23
enable web 80
# STORM
config traffic control 1-5 broadcast disable multicast disable unicast
disable thres
hold 128
# GM
config sim candidate
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

ping

目的

ネットワークデバイス間の接続性をテストします。

構文

ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}

説明

Ping コマンドはリモート IP アドレスに Internet Control Message Protocol（ICMP）エコーメッセージを送信します。その後、リモート IP アドレスは、「エコー」するか、またはメッセージを返します。これは、スイッチとリモートデバイス間の接続性を確認するために使用されます。

パラメータ

パラメータ	説明
<ipaddr>	ホストの IP アドレスを指定します。
times <value 1-255>	送信する各 ICMP エコーメッセージ数。0 の値は ICMP エコーメッセージを継続的に送信します。最大値は 255 です。初期値は 0 です。
timeout <sec 1-99>	リモートデバイスからの応答を待つ時間を定義します。1-99（秒）を指定します。初期値は 1（秒）です。

制限事項

なし。

使用例

IP アドレス 10.48.74.121 に 4 回 ping します。

```
DES-3526:admin#ping 10.48.74.121 times 4
Command: ping 10.48.74.121

Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms

Ping Statistics for 10.48.74.121
Packets: Sent =4, Received =4, Lost =0

DES-3526:admin#
```

enable autoconfig

目的

スイッチの自動コンフィグレーション機能を起動します。現在使用するために、保存済みのコンフィグレーションファイルがロードされます。

構文

enable autoconfig

説明

autoconfig がスイッチで有効にされると、DHCP リプライにはコンフィグレーションファイルとパス名が含まれます。その後、リプライで指定された TFTP サーバからファイルをリクエストします。autoconfig が有効にされると、ipif 設定は自動的に DHCP クライアントになります。

パラメータ

なし。

制限事項

autoconfig が有効にされると、スイッチは自動的に DHCP クライアントになります。(「config ipif <ipif_name12> dhcp」コマンドと同様。) DHCP サーバは、TFTP サーバの IP アドレスとコンフィグレーションファイル名を持ち、DHCP 応答パケットのデータフィールド内にこの情報を提供するように設定される必要があります。TFTP サーバは、スイッチからリクエストを受信する時に動作し、ベースディレクトリ内にリクエストされたコンフィグレーションファイルを持つ必要があります。コンフィグレーションファイルのロードに関する情報については DHCP サーバと TFTP サーバソフトウェアの説明書を参照してください。スイッチが自動コンフィグレーション処理を完了できないと、スイッチメモリ内の以前に保存されたローカルなコンフィグレーションファイルがロードされます。
管理者レベルまたはオペレータレベルユーザのみ本コマンドを実行できます。

注意 DHCP/TFTP サーバユーティリティソフトウェアは、そのユーザインタフェースによってはコンフィグレーションファイル名とパスのエントリを必要とする可能性があります。また、DHCP ソフトウェアは、コンフィグレーションファイル名とパスを持つ個別の ext ファイルをサーバの指定ディレクトリに作成することが必要な場合があります。不明確である場合、DCHP サーバソフトウェアのドキュメントを参照してください。

使用例

スイッチの自動コンフィグレーションを有効にします。

```
DES-3526:admin#enable autoconfig
Command: enable autoconfig

Success.

DES-3526:admin#
```

autoconfig が有効になると、スイッチは再起動され、autoconfig リクエスト（例 : download configuration）の初期化が行われます。しばらくすると、通常のログイン画面が表示されます。その後、コンソールは、DHCP サーバまたは TFTP サーバで指定された設定ファイルからロードされるコンフィグレーションパラメータを表示します。これは「download cfg_fromTFTP」コマンドを使用するのと同じです。全体のスイッチコンフィグレーションがロードされると、スイッチは自動的にサーバを「ログアウト」します。コンフィグレーション設定は、自動的に保存され、アクティブなコンフィグレーションになります。

注意 autoconfig 機能がエラーになると、警告メッセージが表示され、スイッチはコンフィグレーション設定をアップロードしません。

起動時に autoconfig 処理は初期化され、コンソール画面は以下の例と同様に表示されます。コンフィグレーション設定は通常の順序でロードされます。

```
                DES-3526 Fast Ethernet Switch Command Line Interface

                Firmware: Build 5.01-B19
     Copyright(C) 2008 D-Link Corporation.All rights reserved.

DES-3526:admin#
DES-3526:admin#
DES-3526:admin#download config 10.41.44.44 c:\cfg\setting.txt
Command: download config 10.41.44.44 c:\cfg\setting.txt

Connecting to server...................Done.
Download configuration.................Done.
```

ログアウトを含む auto_config プロセスの最後には、以下のように表示されます。

```
DES-3526:admin#create iproute default 172.18.212.253 1
Command: create iproute default 172.18.212.253 1

Success.

DES-3526:admin#
DES-3526:admin##-------------------------------------------------
DES-3526:admin## End of configuration file for DES-3526
DES-3526:admin#

**********
*Logout*
**********
```

注意 autoconfig が有効な場合、スイッチの ipif 設定は、DHCP クライアントとしてスイッチを定義します。「show switch」コマンドは、新しい IP 設定ステータスを表示します。

disable autoconfig

目的

DHCP から自動コンフィグレーション設定を無効にします。

構文

disable autoconfig

説明

DHCP サーバから自動コンフィグレーション指示を受けないようにします。これはスイッチの IP 設定を変えるものではありません。ipif 設定は「config ipif」コマンドで変更されるまで、DHCP クライアントとして継続します。

パラメータ

なし。

制限事項

管理者レベルまたはオペレータレベルユーザのみ本コマンドを実行できます。

使用例

自動コンフィグレーション機能を無効にします。

```
DES-3526:admin#disable autoconfig
Command: disable autoconfig

Success.

DES-3526:admin#
```

show autoconfig

目的

スイッチの現在の autoconfig ステータスを表示します。

構文

show autoconfig

説明

自動コンフィグレーション機能の現在のステータスを示します。

パラメータ

なし。

制限事項

管理者レベルまたはオペレータレベルユーザのみ本コマンドを実行できます。

使用例

自動コンフィグレーションステータスを参照します。

```
DES-3526:admin#show autoconfig
Command: show autoconfig
Autoconfig disabled.

Success.

DES-3526:admin#
```

show firmware information

目的

ファームウェアセクション情報を表示します。

構文

show firmware information

説明

ファームウェアセクション情報を表示します。

パラメータ

なし。

制限事項

なし。

使用例

自動コンフィグレーション機能を無効にします。

```
DES-3526:admin#show firmware information
Command: show firmware information

ID  Version   Size(B)  Update Time          From                User
--  --------  -------  -------------------  ------------------  ---------------
*1  4.00.B55  5132493  2008/05/19 12:54:23  10.90.90.1          admin
 2  4.00.B55  5132493  2008/05/19 13:01:04  10.90.90.1          admin

'*' means boot up section
(T) means firmware update through TELNET
(S) means firmware update through SNMP
(W) means firmware update through WEB
(SIM) means firmware update through Single IP Management

Free space: 0 bytes

DES-3526:admin#
```

第 9 章　ネットワークモニタリングコマンド

コマンドラインインタフェース（CLI）におけるネットワークモニタリングコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
show packet ports	<portlist>
show error ports	<portlist>
show utilization	[cpu | ports {<portlist>}]
clear counters	ports <portlist>
clear log	
show log	index <value>
enable syslog	
disable syslog	
show syslog	
create syslog host	<index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number>| state [enable | disable]
config syslog host	[all | <index 1-4>] {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]}
delete syslog host	[<index 1-4> | all]
show syslog host	<index 1-4>
config system_severity	[trap | log | all] [critical | warning | information]
show system_severity	

次のセクションから各コマンドについて詳しく説明します。

show packet ports

目的

スイッチが送受信したパケットに関する統計情報を表示します。

構文

show packet ports <portlist>

説明

<portlist> で指定されたポートごとに送受信されたパケットに関する統計情報を表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例：1:1-1:3,1:7-1:9）

制限事項

なし。

使用例

ポート 1 のパケット分析を表示します。

```
DES-3526:admin#show packet ports 1
Command: show packet ports 1

Port number : 1
Frame Size    Frame Counts  Frames/sec    Frame Type  Total       Total/sec
------------  ------------  ----------    ----------  ----------  ---------
64            0             0             RX Bytes    0           0
65-127        0             0             RX Frames   0           0
128-255       0             0
256-511       0             0             TX Bytes    0           0
512-1023      0             0             TX Frames   0           0
1024-1518     0             0

Unicast RX    0             0
Multicast RX  0             0
Broadcast RX  0             0
```

show error ports

目的

ポート範囲のエラー統計情報を表示します。

構文

show error ports <portlist>

説明

スイッチが指定ポートに対して収集し、ログ取得を行ったすべてのパケットエラー統計情報を表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例：1:1-1:3,1:7-1:9）

制限事項

なし。

使用例

ポート 1 のエラーを表示します。

```
DES-3526:admin# show error ports 1
Command: show error ports 1

Port number : 1
                RX Frames                                   TX Frames
                ----------                                  ----------
CRC Error       0                   Excessive Deferral      0
Undersize       0                   CRC Error               0
Oversize        0                   Late Collision          0
Fragment        0                   Excessive Collision     0
Jabber          0                   Single Collision        0
Drop Pkts       0                   Collision               0
```

show utilization

目的

リアルタイムにポートと CPU の使用率統計情報を表示します。

構文

show utilization [cpu | ports {<portlist>}]

説明

スイッチのリアルタイムにスイッチのポートと CPU の使用率統計情報を表示します。

パラメータ

パラメータ	説明
ports<portlist>	スイッチの現在のポート使用率を表示します。 <portlist> - 表示されるポートやポート範囲を設定します。
cpu	スイッチの現在の CPU 使用率を表示します。

制限事項

なし。

使用例

ポート使用率の統計情報を表示します。

```
DES-3526:admin#show utilization ports
Command: show utilization ports

Port    TX/sec      RX/sec      Util    Port    TX/sec      RX/sec      Util
------  ----------  ----------  ----    ------  ----------  ----------  ----
1       0           0           0       22      0           0           0
2       0           0           0       23      0           0           0
3       0           0           0       24      0           0           0
4       0           0           0       25      0           0           0
5       0           0           0       26      0           0           0
6       0           0           0
7       0           0           0
8       0           0           0
9       0           0           0
10      0           0           0
11      0           0           0
12      0           0           0
13      0           0           0
14      0           0           0
15      0           0           0
16      0           0           0
17      0           0           0
18      0           0           0
19      0           0           0
20      0           0           0
21      0           0           0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

現在の CPU 使用率を表示します。

```
DES-3526:admin#show utilization cpu
CPU utilization : show utization cpu
--------------------------------------------------------------------------------
Five seconds - 6%        One minute - 13%         Five minutes - 1%


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

clear counters

目的

スイッチの統計情報カウンタをクリアします。

構文

clear counters {ports <portlist>}

説明

統計情報を編集するために、スイッチが使用するカウンタをクリアします。

パラメータ

パラメータ	説明
ports <portlist>	表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

カウンタをクリアします。

```
DES-3526:admin#clear counters ports 1
Command: clear counters ports 1

Success.

DES-3526:admin#
```

clear log

目的

スイッチのヒストリログをクリアします。

構文

clear log

説明

スイッチのヒストリログをクリアします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

ログ情報をクリアします。

```
DES-3526:admin#clear log
Command: clear log

Success.

DES-3526:admin#
```

show log

目的
スイッチのヒストリログを表示します。
構文
show log {index <value>}
説明
スイッチのヒストリログの内容を表示します。
パラメータ

パラメータ	説明
index <value>	フィールドで 1 から始まり、ユーザに指定された値で終わるヒストリログを表示します。 パラメータを指定しないと、すべてのヒストリログエントリを表示します。

制限事項
なし。
使用例
スイッチのヒストリログの内容を表示します。

```
DES-3526:admin#show log index 1
Command: show log index 1

Index  Time                 Log Text
-----  -------------------  ------------------------------------------------------
1      2008/05/19 12:46:13  Configuration and log saved to flash by console (Use
                            rname: Anonymous)
```

enable syslog

目的
システムログがリモートホストに送信される機能を有効にします。
構文
enable syslog
説明
システムログがリモートホストに送信される機能を有効にします。
パラメータ
なし。
制限事項
管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。
使用例
スイッチの Syslog 機能を有効にします。

```
DES-3526:admin#enable syslog
Command: enable syslog

Success.

DES-3526:admin#
```

disable syslog

目的
システムログがリモートホストに送信される機能を無効にします。
構文
disable syslog
説明
システムログがリモートホストに送信される機能を無効にします。
パラメータ
なし。
制限事項
管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。
使用例
スイッチの Syslog 機能を無効にします。

```
DES-3526:admin#disable syslog
Command: disable syslog

Success.

DES-3526:admin#
```

show syslog

目的
Syslog 機能のグローバルに動作中のステータスを表示します。
構文
show syslog
説明
スイッチの Syslog 機能について現在の動作状態を表示します。
パラメータ
なし。
制限事項
なし。
使用例
Syslog 機能のグローバルな状態を表示します。

```
DES-3526:admin#show syslog
Command: show syslog

Syslog Global State: Disabled

DES-3526:admin#
```

create syslog host

目的
新しい Syslog ホストを作成します。
構文
create syslog host <index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]}
説明
新しい Syslog ホストを作成します。
パラメータ

パラメータ	説明	
index <1-4>	コマンドを適用する Syslog ホストのインデックスを指定します。1-4 の 4 つのインデックスが利用可能です。	
ipaddress <ipaddr>	Syslog メッセージを送信されるリモートホストの IP アドレスを指定します。	
severity [informational | warning | all]	3 つの Severity レベル（メッセージレベル）をサポートしています。	
	メッセージレベル	説明
	informational warning all	情報メッセージをリモートホストに送信します。 警告メッセージをリモートホストに送信します。 スイッチに生成される現在サポートしている Syslog メッセージのすべてをリモートホストに送信します。
facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7]	いくつかのオペレーティングシステムデーモンおよびプロセスはファシリティ値を割り当てられています。ファシリティを割り当てていないプロセスとデーモンの場合は「local use」（アプリケーション用の汎用）のいずれかを使用するか、「user-level」を使用します。指定できるファシリティは以下の通りです。	
	コード	ファシリティ
	local0 local1 local2 local3 local4 local5 local6 local7	ローカル使用 0（local 0） ローカル使用 1（local 1） ローカル使用 2（local 2） ローカル使用 3（local 3） ローカル使用 4（local 4） ローカル使用 5（local 5） ローカル使用 6（local 6） ローカル使用 7（local 7）
udp_port <udp_port_number>	Syslog プロトコルがメッセージをリモートホストに送信するために使用する UDP ポート番号（514 または 6000-65535）を指定します。	
state [enable | disable]	リモートホストへの Syslog メッセージの送信を「enable」（有効）または「disable」（無効）にします。	

制限事項
管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。
使用例
Syslog ホストを作成します。

```
DES-3526:admin#create syslog host 1 ipaddress 10.1.1.1 state enable
Command: create syslog host 1 ipaddress 10.1.1.1 state enable

Success.

DES-3526:admin#
```

config syslog host

目的

Syslog プロトコルを設定し、システムログデータをリモートホストに送信します。

構文

config syslog host [all<index 1-4>] [severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]]

説明

Syslog プロトコルを設定し、システムログ情報をリモートホストに送信します。

パラメータ

<table>
<tr><th>パラメータ</th><th colspan="2">説明</th></tr>
<tr><td>[all <index 1-4>]</td><td colspan="2">・all - 全てのホストを指定します。
・ <index 1-4> - コマンドを適用する Syslog ホストのインデックスを指定します。1-4 の 4 つのインデックスが利用可能です。</td></tr>
<tr><td rowspan="3">severity [informational | warning | all]</td><td colspan="2">3 つの Severity レベル（メッセージレベル）をサポートしています。</td></tr>
<tr><td>メッセージレベル</td><td>説明</td></tr>
<tr><td>・informational
・warning
・all</td><td>情報メッセージをリモートホストに送信します。
警告メッセージをリモートホストに送信します。
スイッチに生成される現在サポートしている Syslog メッセージのすべてをリモートホストに送信します。</td></tr>
<tr><td rowspan="3">facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7]</td><td colspan="2">いくつかのオペレーティングシステムデーモンおよびプロセスはファシリティ値を割り当てられています。ファシリティを割り当てていないプロセスとデーモンの場合は「local use」（アプリケーション用の汎用）のいずれかを使用するか、「user-level」を使用します。指定できるファシリティは以下の通りです。</td></tr>
<tr><td>コード</td><td>ファシリティ</td></tr>
<tr><td>local0
local1
local2
local3
local4
local5
local6
local7</td><td>ローカル使用 0（local 0）
ローカル使用 1（local 1）
ローカル使用 2（local 2）
ローカル使用 3（local 3）
ローカル使用 4（local 4）
ローカル使用 5（local 5）
ローカル使用 6（local 6）
ローカル使用 7（local 7）</td></tr>
<tr><td>udp_port <udp_port_number></td><td colspan="2">Syslog プロトコルがメッセージをリモートホストに送信するために使用する UDP ポート番号を指定します。</td></tr>
<tr><td>ipaddress <ipaddr></td><td colspan="2">Syslog メッセージを送信されるリモートホストの IP アドレスを指定します。</td></tr>
<tr><td>state [enable | disable]</td><td colspan="2">リモートホストへの Syslog メッセージの送信を「enable」（有効）または「disable」（無効）にします。</td></tr>
</table>

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

Syslog ホストを設定します。

```
DES-3526:admin#config syslog host 1 severity all
Command: config syslog host 1 severity all

Success.
```

```
DES-3526:admin#config syslog host 1 facility local0
Command: config syslog host 1 facility local0

Success.
```

すべての Syslog ホストを設定します。

```
DES-3526:admin#config syslog host all severity all
Command: config syslog host all severity all

Success.
```

```
DES-3526:admin#config syslog host all facility local0
Command: config syslog host all facility local0

Success.
```

delete syslog host

目的

設定した Syslog ホストをスイッチから削除します。

構文

delete syslog host [<index 1-4> | all]

説明

スイッチから定義済みの Syslog ホストを削除します。

パラメータ

パラメータ	説明
<index 1-4>	コマンドを適用する Syslog ホストのインデックスを指定します。1-4 の 4 つのインデックスが利用可能です。
all	すべてのホストに本コマンドを適用します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

定義済みの Syslog ホストを削除します。

```
DES-3526:admin#delete syslog host 4
Command: delete syslog host 4

Success.

DES-3526:admin#
```

show syslog host

目的

スイッチに現在設定されている Syslog ホストを表示します。

構文

show syslog host {<index 1-4>}

説明

スイッチに設定されている Syslog ホストを表示します。

パラメータ

パラメータ	説明
<index 1-4>	コマンドを適用する Syslog ホストのインデックスを指定します。1-4 の 4 つのインデックスが利用可能です。

制限事項

なし。

使用例

Syslog ホスト情報を表示します。

```
DES-3526:admin#show syslog host
Command: show syslog host

Syslog Global State: Disabled

Host Id  Host IP Address     Severity     Facility  UDP port   Status
-------  ---------------  --------------  --------  --------  --------
1        10.1.1.1         All             Local0    514       Enabled

Total Entries : 1

DES-3526:admin#
```

config system_severity

目的

ログエントリまたはトラップメッセージに必要とされるアラートのメッセージレベルを設定します。

構文

config system_severity [trap | log | all] [critical | warning | information]

説明

本コマンドは、スイッチのシステムメッセージレベルを設定します。イベントがスイッチに発生する時、SNMP エージェント（トラップ）、スイッチのログまたは両方にメッセージは送信されます。スイッチに発生するイベントは 3 つの主なカテゴリに分けられます。これらのカテゴリは同じ名前のパラメータと厳密には同じではありません（以下参照）。

- information - information として分類されるイベントは、スイッチの様々な機能を有効または無効にするなどの問題とは見なされないようなスイッチにおける基本的なイベントです。
- warning - warning として分類されるイベントは、ダウンロード / アップロードの失敗やログインの失敗などスイッチの全般的な機能にとって総括的機能に重要でないが、注意を必要とする問題の多いイベントです。
- critical - critical として分類されるイベントは、ハードウェアの故障やスプーフィング攻撃などのスイッチに発生する致命的なイベントです。

パラメータ

以下のパラメータから 1 つを選び、送信されるシステムメッセージレベルを指定します。

パラメータ	説明
trap	スイッチに発生するどのイベントが分析のために SNMP エージェントに送られるかを定義します。
log	スイッチに発生するどのイベントが分析のためにスイッチのログに送信されるかを定義します。
all	スイッチに発生するどのイベントが分析のために SNMP エージェントとスイッチのログに送られるかを定義します。

以下のパラメータから 1 つを選び、どのシステム警告レベルが上で入力された宛先に送信されるかを指定します。

パラメータ	説明
critical	上で記述したように適切な宛先とともに本パラメータを入力すると、本スイッチのログまたは SNMP エージェントに critical イベントだけを送付します。
warning	上で記述したように適切な宛先とともに本パラメータを入力すると、本スイッチのログまたは SNMP エージェントに warning イベントおよび critical イベントを送付します。
information	上で記述したように適切な宛先とともに本パラメータを入力すると、本スイッチのログまたは SNMP エージェントに informational イベント、warning イベントおよび critical イベントを送付します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

システムメッセージレベル設定を重要なトラップにだけ設定します。

```
DES-3526:admin#config system_severity trap critical
Command: config system_severity trap critical

Success.

DES-3526:admin#
```

show system_severity

目的

スイッチの現在のシステムメッセージレベルを表示します。

構文

show system_severity

説明

「config system_severity」コマンドを使用してスイッチに行ったシステムメッセージレベルを参照します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチの現在のシステムメッセージレベル設定を参照します。

```
DES-3526:admin#show system_severity
Command: show system_severity

System Severity
--------------------
Log  : information
Trap : critical

DES-3526:admin#
```

第 10 章　マルチプルスパニングツリー（MSTP）コマンド

本スイッチは 3 つのバージョンのスパニングツリープロトコル（802.1D STP、802.1w Rapid STP、802.1s MSTP）をサポートしています。MSTP（Multiple Spanning Tree Protocol）は IEEE 委員会により定義された標準規格で、複数の VLAN を 1 つのスパニングツリーインスタンスにマッピングし、ネットワーク中に複数の経路を提供します。また、ロードバランシングを可能にし、1 つのインスタンスに障害が発生した場合でも、広い範囲で影響を与えないようにすることができます。障害発生時には障害が発生したインスタンスに代わって新しいトポロジを素早く収束します。これら VLAN 用のフレームは、これらの 3 つのスパニングツリープロトコル（STP、RSTP、MSTP）のいずれかを使用して、素早く適切に相互接続されたブリッジを通して処理されます。本プロトコルでは、BPDU（Bridge Protocol Data Unit）パケットにタグ付けを行い、受信するデバイスが、スパニングツリーインスタンス、スパニングツリーリージョン、およびそれらに関連付けられた VLAN を区別できるようにしています。これらのインスタンスは Instance_ID によって分類されます。MSTP では、複数のスパニングツリーを CIST（Common and Internal Spanning Tree）で接続します。CIST は自動的に各 MSTP リージョンとその最大範囲を決定し、1 つのスパニングツリーを構成する 1 つの仮想ブリッジのように見せかけます。そのため、異なる VLAN を割り当てられたフレームは、ネットワーク上の管理用に設定されたリージョン中の異なるデータ経路を通ります。ネットワーク上の MSTP を使用しているスイッチは、以下の 3 つの属性を持つ 1 つの MSTP 構成を持ちます。

a）32 文字までの半角英数字で定義された「Configuration 名」（「config stp mst_config_id」コマンドでの name <string> として設定済み）。
b）「Configuration Revision 番号」（「Revision Level」として設定済み）。
c）4096 件のエレメントテーブル（「VID range」として設定済み）。スイッチがサポートする 4096 件までの VLAN とインスタンスとの関連付けです。

スイッチで MSTP 機能を利用するためには、以下の手順を実行します。

a）スイッチに MSTP 設定を行います（「config stp version」コマンド）。
b）MSTP インスタンスに適切なスパニングツリープライオリティを設定します（「config stp priority」コマンド）。
c）共有する VLAN を MSTP Instance ID に追加する必要があります（「config stp instance_id」コマンド）。

コマンドラインインタフェース（CLI）におけるマルチプルスパニングツリーコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable stp	
disable stp	
config stp version	[mstp | rstp | stp]
config stp	{maxage <value 6-40> | maxhops <value 1-20> | hellotime <value 1-2> | forwarddelay <value 4-30>| txholdcount <value 1-10> | fbpdu [enable | disable]}
config stp ports	<portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | restricted_tcn [true | false] | restricted_role [true | false] | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable |disable]}
create stp instance_id	<value 1-4>
config stp instance _id	<value 1-4> [add_vlan | remove_vlan] <vidlist>
delete stp instance_id	<value 1-4>
config stp priority	<value 0-61440> instance_id <value 0-4>
config stp mst_config_id	{revision_level <int 0-65535> | name <string>}
config stp mst_ports	<portlist> instance_id <value 0-4> {internalCost [auto | value 1-200000000] | priority <value 0-240>}
show stp	
show stp ports	{<portlist>}
show stp instance	{<value 0-4>}
show stp mst_config id	

次のセクションから各コマンドについて詳しく説明します。

enable stp

目的
スイッチの STP をグローバルに有効にします。
構文
enable stp
説明
スイッチの STP をグローバルに有効にします。
パラメータ
なし。
制限事項
管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。
使用例
スイッチの STP をグローバルに有効にします。

```
DES-3526:admin#enable stp
Command: enable stp

Success.

DES-3526:admin#
```

disable stp

目的
スイッチの STP をグローバルに無効にします。
構文
disable stp
説明
スイッチの STP をグローバルに無効にします。
パラメータ
なし。
制限事項
管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。
使用例
スイッチの STP をグローバルに無効にします。

```
DES-3526:admin#disable stp
Command: disable stp

Success.

DES-3526:admin#
```

config stp version

目的
スイッチの STP バージョンをグローバルに設定します。
構文
config stp version [mstp | rstp | stp]
説明
スイッチで実行する STP バージョンを選択します。
パラメータ

パラメータ	説明
mstp	スイッチ上で MSTP がグローバルに使用されます。
rstp	スイッチ上で RSTP がグローバルに使用されます。
stp	スイッチ上で STP がグローバルに使用されます。

制限事項
管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。
使用例
スイッチに MSTP をグローバルに設定します。

```
DES-3526:admin#config stp version mst
Command: config stp version mstp

Success.

DES-3526:admin#
```

config stp

目的

スイッチに STP、RSTP、および MSTP を設定します。

構文

config stp {maxage <value 6-40>|maxhops <value 6-40> |hellotime <value 1-2>|forwarddelay <value 4-30>|txholdcount <value 1-10>|fbpdu [enable|disable]}

説明

スイッチに STP を設定します。すべてのコマンドが現在スイッチに設定されている STP バージョンに対して実行されます。

パラメータ

パラメータ	説明
maxage <value 6-40>	本値は古い情報がネットワーク内の冗長パスを永遠に循環し、新しい有効な情報伝播の妨害を避けるために設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN（ブリッジで相互接続された LAN）内のデバイスが持っているスパニングツリー設定値が矛盾していないかを確認するための値です。本値が経過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。6-40（秒）の範囲から指定します。初期値は 200 です。
maxhops <value 6-40>	スイッチが送信した BPDU パケットが破棄される前のスパニングツリー範囲内のデバイス間のホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。スイッチは、その後 BDPU パケットを破棄し、ポートに保持していた情報を解放します。ホップカウントは 1-20 で指定します。初期値は 20 です。
hellotime <value 1-2>	STP のルートデバイス、または RSTP の代表ルータによるコンフィグレーションメッセージの送信間隔を 1-2（秒）で設定します。このようにして、スイッチがまだ機能していることをと通知します。初期値は 2（秒）です。MSTP では、スパニングツリーがポートごとに設定されるため、MSTP を使用するスイッチには「config stp ports」コマンドを使用して hellotime が設定される必要があります。
forwarddelay <value 4-30>	状態を変更する前にルートデバイスが待機する最大時間（4-30 秒）。初期値は 15（秒）です。
txholdcount <value 1-10>	間隔ごとに送信される BPDU Hello パケットの最大数。初期値は 3（秒）です。
fbpdu [enable | disable]	STP を無効にすると、STP BPDU パケットが他のネットワークデバイスから送信されます。初期値は「enable」です。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

「maxage」が 18、「maxhops」が 15 の STP を設定します。

```
DES-3526:admin#config stp maxage 18 maxhops 15
Command: config stp maxage 18 maxhops 15

Success.

DES-3526:admin#
```

config stp ports

目的

ポートレベルで STP を設定します。

構文

config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | restricted_tcn [true | false] | restricted_role [true | false] | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable |disable]}

説明

ポートのグループに STP を作成し、設定します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）
externalCost [auto | <value 1-200000000>]	設定対象のポートに対し、パケット送信のためのコストを表すメトリックを定義します。ポートコストは、自動設定、あるいは手動でメトリック値を指定できます。初期値は「auto」です。 • auto - 指定したポートに対して、最適なパケット送信スピードを自動的に設定します。デフォルトポートコスト : 100Mbps ポートの場合は 200000、ギガビットポートの場合は 20000。 • <value 1-200000000> - 1-200000000 の範囲から指定します。小さい数字を指定すると、パケット送出ポートとして選出される確率が上がります。
hellotime <value 1-2>	指定ポートが Bridged LAN（ブリッジにより接続される LAN）上の他のデバイスに Configuration メッセージを送信する間隔。このようにして、スイッチがまだ機能していることをと通知します。1-2（秒）の範囲から指定します。初期値は 2（秒）です。
migrate [yes | no]	「yes」を設定すると、STP 設定に関する情報をリクエストする他のブリッジに BPDU パケットをポートが送信するように設定します。スイッチが RSTP に設定されると、ポートは 802.1D STP から 802.1w RSTP まで移行することができます。スイッチが MSTP に設定されると、ポートは 802.1D STP から 802.1MSTP まで移行することができます。RSTP と MSTP は標準の STP と共存できますが、RSTP と MSTP の利点は 802.1D ネットワークが 802.1w または 802.1s が有効なネットワークに接続するポート上では実現されません。セグメントのすべてまたは一部において 802.1w RSTP または 802.1s にアップグレード可能なネットワークステーションまたはセグメントに接続したポートでは本パラメータを「yes」とします。
edge [true | false | auto]	• true - 選択ポートをエッジポートとして指定します。しかし、トポロジの変更によってループ発生の可能性が生じると、エッジポートはエッジポートとしての資格を失います。エッジポートは通常 BPDU パケットを受け取りません。もし、BPDU パケットが受信されると、そのポートはエッジポートの資格を失います。 • false - そのポートにエッジポートの資格がないことを示しています。 • auto - 選択ポートは可能な時にエッジポートとして指定されます。
restricted_tcn [true | false]	管理者によって設定されるブーリアン値。「True」と「False」の 2 つのオプションが使用できます。初期値は false です。 • True - ポートは受信したトポロジ変更通知およびトポロジ変更を他のポートに伝搬しません。 • False - 不正確に学習したステーションの位置情報によって、スパニングツリーのアクティブなトポロジ変更の後に一時的な接続性の低下を引き起こす可能性があります。ブリッジすると、管理者のフルコントロール下または接続している LAN の頻繁な遷移への MAC 操作のフルコントロール下ではなくなる可能性があるため、コア部分内でアドレスのフラッシュを引き起こすネットワークのコア部分の外側にはブリッジしないように設定します。
restricted_role [true | false]	管理者によって設定されるブーリアン値。「True」と「False」の 2 つのオプションが使用できます。初期値は false です。 • True - 最適なスパニングツリー優先度ベクトルを持っていてもポートは、CIST またはすべての MSTI のルートポートとして選択されなくなります。そのようなポートは、ルートポートの選択後に代替ポートとして選択されます。 • False - 設定されると、スパニングツリーの接続性の低下を引き起こす可能性があります。ブリッジすると、管理者のフルコントロール下ではなくなる可能性があるため、スパニングツリーのアクティブなトポロジに影響するネットワークのコア部分の外側にはブリッジしないように設定します。
p2p [true | false | auto]	• true - 選択ポートを P2P ポートとして指定します。P2P ポートはエッジポートと似ていますが、P2P ポートは全二重モードでのみ動作する点で異なります。RSTP の特長は、エッジポート同様、P2P ポートは迅速に Forwarding 状態に遷移します。 • false - そのポートに P2P ポートの資格がないことを示しています。 • auto - ポートはいつでも可能な時に（「true」を指定した時と同様に）P2P ポートとして動作します。 ポートの資格を失う時（例えば、半二重モードを指定された時など）、自動的に「false」を指定した時と同様になります。初期値は「auto」です。
state [enable | disable]	ポートリストに指定されたポートに STP 機能を「enable」（有効）または「disable」（無効）にします。初期値は「enable」です。
fbpdu [enable | disable]	STP を無効にすると、STP BPDU パケットが他のネットワークデバイスから送信されます。STP がグローバルに無効で、BPDU パケットの転送が有効である場合には、本機能は使用中である場合があります。初期値は有効で、BPDU パケットは転送されません。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

モジュール 1 のポート 1-5 に「path cost」が 19、「hellotime」に 5（秒）、「migration」に enable、「state」が enable の STP を設定します。

```
DES-3526:admin#config stp ports 1:1-1:5 externalCost 19 hellotime 5 migrate yes state enable
Command: config stp ports 1:1-1:5 externalCost 19 hellotime 5 migrate yes state enable

Success.

DES-3526:admin#
```

create stp instance_id

目的

MSTP に STP インスタンス ID を作成します。

構文

create stp instance_id <value 1-4>

説明

MSTP に STP インスタンス ID を作成します。スイッチには 16 個のインスタンス（1 つは CIST で変更できません。）があり、4 個のインスタンス ID を作成することができます。

パラメータ

パラメータ	説明
<value 1-4>	スイッチに STP インスタンスを指定するために 1-4 の範囲から指定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

STP インスタンス 2 を作成します。

```
DES-3526:admin#create stp instance_id 2
Command: create stp instance_id 2

Success.

DES-3526:admin#
```

config stp instance_id

目的

STP インスタンス ID の追加または削除をします。

構文

config stp instance_id <value 1-4> [add_vlan | remove_vlan] <vidlist>

説明

スイッチにインスタンス _ID を作成することによって、VID（VLANID）を設定済みの STP インスタンスにマップします。STP インスタンスは、同じ MSTP 設定を持つ複数メンバを持っています。ネットワークにおける、STP 範囲の数には制限はありませんが、各範囲は、最大 16 個の STP インスタンス（1 つは変更できないデフォルトエントリ）をサポートしています。VID は一度に 1 つの STP インスタンスにだけ所属することができます。同様に同じ STP インスタンス _ID を持つ同じ STP 範囲にあるスイッチがマップされ、同じ設定のリビジョンレベル番号と同じ名前を持つ必要があることに注意してください。

パラメータ

パラメータ	説明
<value 1-4>	スイッチに STP インスタンスを指定するために 1-4 の範囲から指定します。スイッチは 0 として設定されている変更できないデフォルト・インスタンス ID を含め 16 個の STP 範囲をサポートしています。
add_vlan	<vidlist> パラメータと共に、設定済みの STP インスタンス ID に VID を追加します。
remove_vlan	<vidlist> パラメータと共に、設定済みの STP インスタンス ID から VID を削除します。
<vidlist>	スイッチに登録済みの VLAN の中から、VID の範囲（1-4094）を指定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

インスタンス ID 2 を設定し、VID 10 を追加します。

```
DES-3526:admin#config stp instance_id 2 add_vlan 10
Command: config stp instance_id 2 add_vlan 10

Success.

DES-3526:admin#
```

インスタンス ID2 から VID 10 を削除します。

```
DES-3526:admin#config stp instance_id 2 remove_vlan 10
Command: config stp instance_id 2 remove_vlan 10

Success.

DES-3526:admin#
```

delete stp instance_id

目的

スイッチから設定済みの STP インスタンス ID を削除します。

構文

delete stp instance_id <value 1-4>

説明

スイッチから設定済みの STP インスタンス ID を削除します。

パラメータ

パラメータ	説明
<value 1-4>	スイッチに STP インスタンス（1-4）を指定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチからインスタンス ID 2 を削除します。

```
DES-3526:admin#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DES-3526:admin#
```

config stp priority

目的

STP インスタンス設定を更新します。

構文

config stp priority <value 0-61440> instance_id <value 0-4>

説明

スイッチの STP インスタンス設定を更新します。MSTP は、ルートブリッジ、ルートポート、および代表ポートを選択するために優先度を使用します。STP 範囲により高いプライオリティを割り当てることで、送信パケットのための選択された instance_id に優先権を付与します。数字が低いほど、優先度は高くなります。

パラメータ

パラメータ	説明
priority <value 0-61440>	0-61440 の値を選択し、送信パケットに対して指定されたインスタンス ID に優先度を指定します。数字が低いほど、優先度は高くなります。このエントリは 4096 の倍数とする必要があります。
instance_id <value 0-4>	優先度値を設定するためには、希望する設定済みのインスタンス ID に対応する値を入力します。インスタンス ID 0 は、スイッチの内部に設定されているデフォルトのインスタンス ID（CIST）です。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

instance_id 2 に対する優先度値に 4096 を指定します。

```
DES-3526:admin#config stp priority 4096 instance_id 2
Command: config stp priority 4096 instance_id 2

Success.

DES-3526:admin#
```

config stp mst_config_id

目的

MSTP 設定 ID を更新します。

構文

config stp mst_config_id {revision_level <int 0-65535> | name <string 32>}

説明

現在スイッチに設定されている MSTP 設定を編集します。ここに入力された情報は、それが属する MSTP 範囲の識別子として BPDU パケットに添付されます。同じ revision_level と名前を持つスイッチは、同じ MSTP 範囲の一部であると見なされます。

パラメータ

パラメータ	説明
revision_level <int 0-65535>	0-65535 の値を入力し、MSTP 範囲を識別します。本値は name と共に、スイッチに設定した MSTP リージョンを識別します。初期値は 0 です。
name <string 32>	32 文字以内の半角英数字の文字列を入力して、スイッチの MSTP 範囲を識別します。本値は revision_level と共に、スイッチに設定した MSTP リージョンを識別します。name が入力されないと、デフォルト名はデバイスの MAC アドレスになります。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

revision_level 10 と name「ZIra」を持つスイッチの MSTP 範囲を設定します。

```
DES-3526:admin#config stp mst_config_id revision_level 10 name ZIra
Command: config stp mst_config_id revision_level 10 name ZIra

Success.

DES-3526:admin#
```

config stp mst_ports

目的

MSTP インスタンスのポート設定を更新します。

構文

config stp mst_ports <portlist> instance_id <value 0-4> {internalCost [auto | <value 1-200000000>] priority <value 0-240>}

説明

STP instance_id のポート設定を更新します。ループが発生すると、MSTP 機能はポートプライオリティを使用して、Forwarding 状態に遷移させるインタフェースを選択します。最初に選択させたいインタフェースには高いプライオリティ（小さい数値）を与え、最後に選択させたいインタフェースには低いプライオリティ（大きい数値）を与えます。プライオリティ値が同じインスタンスでは、MSTP 機能は最小のポート番号を Forwarding 状態にし、他のインタフェースをブロックします。低優先度値がフォワーディングパケットのために、より高いプライオリティを意味することにご注意ください。

パラメータ

パラメータ	説明
<portlist>	設定するポートまたはポート範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）
instance_id <value 0-4>	スイッチに設定済みの instance_id を識別するために 0-4 の範囲から指定します。0 のエントリは CIST（Common and Internal Spanning Tree）を示します。
internalCost [auto | <value 1-200000000>]	インタフェースが STP インスタンス内で選択される場合、指定ポートへの送信パケットの相対的なコストを設定します。初期値は「auto」です。次の 2 つのオプションがあります。 • auto - インタフェースに自動的に最適な最速ルートを設定します。初期値はインタフェースのメディアスピードに基づきます。 • 1-2000000 - ループが発生した場合、1-2000000 の範囲の値を持つコストを使用して最速ルートを設定します。コストが小さいほど高速で伝送されます。
priority <value 0-240>	ポートインタフェースのプライオリティを 0-240 の範囲から指定します。最初に選択させたいインタフェースには高いプライオリティ（小さい数値）を与え、最後に選択させたいインタフェースには低いプライオリティ（大きい数値）を与えます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

instance ID を持つモジュール 1 のポート 1、2 に internalCost が「auto」でプライオリティ「0」を持つように指定します。

```
DES-3526:admin#config stp mst_ports 1-2 instance_id 1 internalCost auto priority 0
Command: config stp mst_ports 1-2 instance_id 1 internalCost auto priority 0

Success.

DES-3526:admin#
```

show stp

目的

スイッチの現在の STP 設定を表示します。

構文

show stp

説明

スイッチの現在の STP 設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチの現在の STP 設定を表示します。

- ステータス 1 : STP コンパチブルバージョンで有効にされた STP

```
DES-3526:admin#show stp
Command: show stp

STP Bridge Global Settings
--------------------------
STP Status          :Enabled
STP Version         :STP Compatible
Max Age             :20
Hello Time          :2
Forward Delay       :15
Max Age             :20
TX Hold Count       :3
Forwarding BPDU     :Enabled

DES-3526:admin#
```

- ステータス 2 : RSTP で有効にされた STP

```
DES-3526:admin#show stp
Command: show stp

STP Bridge Global Settings
--------------------------
STP Status          :Enabled
STP Version         :RSTP
Max Age             :20
Hello Time          :2
Forward Delay       :15
Max Age             :20
TX Hold Count       :3
Forwarding BPDU     :Enabled

DES-3526:admin#
```

- ステータス 3 : MSTP で有効にされた STP

```
DES-3526:admin#show stp
Command: show stp

STP Bridge Global Settings
--------------------------
STP Status          :Enabled
STP Version         :MSTP
Max Age             :20
Forward Delay       :15
Max Hops            :20
TX Hold Count       :3
Forwarding BPDU     :Enabled


DES-3526:admin#
```

show stp ports

目的

スイッチの現在の STP ポート設定を表示します。

構文

show stp ports <portlist>

説明

スイッチにおける STP ポート設定と現在実行されている STP ポートの動作状態を表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

なし

使用例

STP にポートを表示します。

```
DES-3526:admin#show stp ports
Command: show stp ports

MSTP Port Information
----------------------
Port Index        : 1     ,  Hello Time: 2 /2 ,  Port STP enabled
Restricted role   : False ,  Restricted TCN : False
External PathCost : Auto/200000   ,  Edge Port : False/No ,  P2P : Auto /Yes
Port Forward BPDU : disabled ,      BPDU Type : RSTP

Msti   Designated Bridge   Internal PathCost  Prio  Status       Role
-----  ------------------  -----------------  ----  -----------  ----------
0      N/A                 200000             128   Disabled     Disabled

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

show stp instance_id

目的

スイッチの STP インスタンス設定を表示します。

構文

show stp instance_id {<value 0-4>}

説明

スイッチの現在の STP インスタンス設定と STP インスタンス動作状態を表示します。

パラメータ

パラメータ	説明
<value 0-4>	スイッチに設定済みのインスタンス ID1-4 の範囲から指定します。エントリ 0 は、スイッチの内部に設定されている CIST に対する STP 設定を表示します。

制限事項

なし。

使用例

スイッチのインスタンス 0（内部 CIST）に対する STP インスタンス設定を表示します。

```
DES-3526:admin#show stp instance_id
Command: show stp instance_id

STP Instance Settings
---------------------------
Instance Type           : CIST
Instance Status         : Disabled
Instance Priority       : 32768(bridge priority : 32768, sys ID ext : 0 )

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

show stp mst_config_id

目的

MSTP の設定情報を表示します。

構文

show stp mst_config_id

説明

現在スイッチに設定されている MSTP 情報を表示します。

パラメータ

なし。

制限事項

なし。

使用例

現在スイッチに設定されている MSTP の設定情報を表示します。

```
DES-3526:admin#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
---------------------------------------------------------------

Configuration Name :00:10:20:33:45:00            Revision Level :0
MSTI ID   Vid list
-------   --------
CIST      1-4094

DES-3526:admin#
```

第 11 章　フォワーディングデータベースコマンド

コマンドラインインタフェース（CLI）におけるレイヤ 2 フォワーディングデータベースコマンドとそのパラメータは以下のとおりです。

コマンド	パラメータ
create fdb	<vlan_name 32> <macaddr> port <port>
create multicast_fdb	<vlan_name 32> <macaddr>
config multicast_fdb	<vlan_name 32> <macaddr> [add | delete] <portlist>
config fdb aging_time	<sec 10-1000000>
delete fdb	<vlan_name 32> <macaddr>
clear fdb	[vlan <vlan_name 32> | port <port> | all]
show multicast_fdb	{vlan <vlan_name 32> | mac_address <macaddr>}
show fdb	{port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}
config multicast port_filtering_mode	[<portlist> | all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]
show multicast port_filtering_mode	{<portlist>}

次のセクションから各コマンドについて詳しく説明します。

create fdb

目的

ユニキャスト MAC アドレスフォワーディングテーブル（データベース）にスタティックなエントリを作成します。

構文

create fdb <vlan_name 32> <macaddr> port <port>

説明

ユニキャスト MAC アドレスフォワーディングテーブル（データベース）にエントリを作成します。

パラメータ

パラメータ	説明
<vlan_name 32>	MAC アドレスが存在する VLAN 名。
<macaddr>	フォワーディングテーブルに追加される MAC アドレス。
port<port>	宛先 MAC アドレスに対応するポート番号を入力します。スイッチはこのポートを通じ、いつも指定されたデバイスにトラフィックを送信します。ポートは、「:」（コロン）で分けることによって、最も下位のスイッチ番号と始めのポート番号によって指定されます。例えば、1:3 はスイッチ番号 1 のポート 3 を表しています。2:4 はスイッチ番号 2 のポート 4 を表しています。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

ユニキャスト MAC FDB エントリを作成します。

```
DES-3526:admin#create fdb default 00-00-00-00-01-02 port 1
Command: create fdb default 00-00-00-00-01-02 port 1

Success.

DES-3526:admin#
```

create multicast_fdb

目的

マルチキャスト MAC アドレスフォワーディング（データベース）にスタティックなエントリを作成します。

構文

create multicast_fdb <vlan_name 32> <macaddr>

説明

マルチキャスト MAC アドレスフォワーディングテーブル（データベース）にエントリを作成します。

パラメータ

パラメータ	説明
<vlan_name 32>	MAC アドレスが存在する VLAN 名。
<macaddr>	フォワーディングテーブルに追加される MAC アドレス。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

マルチキャスト MAC フォワーディングを作成します。

```
DES-3526:admin#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

DES-3526:admin#
```

config multicast_fdb

目的

スイッチのマルチキャスト MAC アドレスフォワーディングデータベースを設定します。

構文

config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>

説明

マルチキャスト MAC アドレスフォワーディングテーブルを設定します。

パラメータ

パラメータ	説明
<vlan_name 32>	MAC アドレスが存在する VLAN 名。
<macaddr>	マルチキャストフォワーディングテーブルに追加される MAC アドレス。
[add | delete]	• add - ポートをテーブルに追加します。 • delete - マルチキャストフォワーディングテーブルからポートを削除します。
<portlist>	表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

マルチキャスト MAC フォワーディングを追加します。

```
DES-3526:admin#config multicast_fdb default 01-00-00-00-00-01 add 1:1-1:5
Command: config multicast_fdb default 01-00-00-00-00-01 add 1:1-1:5

Success.

DES-3526:admin#
```

config fdb aging_time

目的

フォワーディングデータベースのエージングタイムを設定します。

構文

config fdb aging_time <sec 10-1000000>

説明

エージングタイムは、スイッチの学習プロセスに影響します。送信元 MAC アドレスと対応するポート番号で構成されるダイナミックフォワーディングテーブルエントリが、エージングタイム内にアクセスされないと、テーブルから削除されます。エージングタイムは 10-10000000 秒で指定します。初期値は 300（秒）です。エージングタイムが非常に長い場合、古いか既に存在しないダイナミックフォワーディングテーブルエントリとなってしまします。これはスイッチに不正確パケット転送決定を引き起こす可能性があります。しかし、エージングタイムが短すぎると、多くのエントリが非常に早く削除されてしまいます。これは送信元アドレスがフォワーディングテーブルで見つけられないパケットを受信する高い確率をもたらし、その場合、スイッチはすべてのポートにパケットをブロードキャストするため、スイッチが持つ利点の多くを無駄にしてしまいます。

パラメータ

パラメータ	説明
<sec 10-1000000>	MAC アドレスフォワーディングデータベースに対するエージングタイム。10-1000000（秒）。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

FDB エージングタイムを設定します。

```
DES-3526:admin#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DES-3526:admin#
```

delete fdb

目的

スイッチのフォワーディングデータベースのエントリを削除します。

構文

delete fdb <vlan_name 32> <macaddr>

説明

スイッチの MAC アドレスフォワーディングデータベースのエントリを削除します。

パラメータ

パラメータ	説明
<vlan_name 32>	MAC アドレスが存在する VLAN 名。
<macaddr>	マルチキャストフォワーディングテーブルから削除される MAC アドレス。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

パーマネント FDB エントリを削除します。

```
DES-3526:admin#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DES-3526:admin#
```

使用例

マルチキャスト FDB エントリを削除します。

```
DES-3526:admin#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

Success.

DES-3526:admin#
```

clear fdb

目的

すべてのダイナミックに学習された MAC アドレスをスイッチのフォワーディングデータベースから削除します。

構文

clear fdb [vlan <vlan_name 32> | port <port> | all]

説明

スイッチのフォワーディングデータベースにダイナミックに学習されたエントリをクリアします。

パラメータ

パラメータ	説明
vlan <vlan_name 32>	MAC アドレスが存在する VLAN 名。
port <port>	宛先 MAC アドレスに対応するポート番号を入力します。スイッチはこのポートを通じ、いつも指定されたデバイスにトラフィックを送信します。ポートは、「:」（コロン）で分けることによって、最も下位のスイッチ番号と始めのポート番号によって指定されます。例えば、1:3 はスイッチ番号 1 のポート 3 を表しています。2:4 はスイッチ番号 2 のポート 4 を表しています。
all	スイッチのフォワーディングデータベースにあるすべてのダイナミックエントリをクリアします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチの FDB ダイナミックエントリをクリアします。

```
DES-3526:admin#clear fdb all
Command: clear fdb all

Success.

DES-3526:admin#
```

show multicast_fdb

目的

スイッチのマルチキャストフォワーディングデータベースの内容を表示します。

構文

show multicast_fdb {vlan <vlan_name 32> | mac_address <macaddr>}

説明

スイッチにおけるマルチキャスト MAC アドレスフォワーディングデータベースの現在の内容を表示します。

パラメータ

パラメータ	説明
<vlan_name 32>	MAC アドレスが存在する VLAN 名。
<macaddr>	フォワーディングテーブルにある MAC アドレス。

制限事項

なし。

使用例

マルチキャスト MAC アドレステーブルを表示します。

```
DES-3526:admin#show multicast_fdb vlan default
Command: show multicast_fdb vlan default

VLAN Name    :default
MAC Address  :01-00-5E-00-00-00
Egress Ports :1:1-1:5
Mode         :Static

Total Entries :1

DES-3526:admin#
```

show fdb

目的

現在のユニキャスト MAC アドレスフォワーディングデータベースを表示します。

構文

show fdb { port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time | vid <vlanid 1-4094>}

説明

スイッチのフォワーディングデータベースの内容を表示します。

パラメータ

パラメータ	説明
port<port>	宛先 MAC アドレスに対応するポート番号を入力します。スイッチはこのポートを通じ、いつも指定されたデバイスにトラフィックを送信します。ポートは、「:」（コロン）で分けることによって、最も下位のスイッチ番号と始めのポート番号によって指定されます。例えば、1:3 はスイッチ番号 1 のポート 3 を表しています。2:4 はスイッチ番号 2 のポート 4 を表しています。
vlan<vlan_name 32>	MAC アドレスが存在する VLAN 名。
mac_address <macaddr>	フォワーディングテーブルにある MAC アドレス。
static	スタティック MAC アドレス。
aging_time	MAC アドレスフォワーディングデータベースのエージングタイム。
vid <vlanid 1-4094>	表示する VLAN ID を指定します。

制限事項

なし。

使用例

ユニキャスト MAC アドレステーブルを表示します。

```
DES-3526:admin#show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300

VID VLAN Name MAC Address        Port Type
--- --------- -----------------  ---- -------
1   default   00-00-39-34-66-9A  1:10 Dynamic
1   default   00-00-51-43-70-00  1:10 Dynamic
1   default   00-00-5E-00-01-01  1:10 Dynamic
1   default   00-00-74-60-72-2D  1:10 Dynamic
1   default   00-00-81-05-00-80  1:10 Dynamic
1   default   00-00-81-05-02-00  1:10 Dynamic
1   default   00-00-81-48-70-01  1:10 Dynamic
1   default   00-00-E2-4F-57-03  1:10 Dynamic
1   default   00-00-E2-61-53-18  1:10 Dynamic
1   default   00-00-E2-6B-BC-F6  1:10 Dynamic
1   default   00-00-E2-7F-6B-53  1:10 Dynamic
1   default   00-00-E2-82-7D-90  1:10 Dynamic
1   default   00-00-F8-7C-1C-29  1:10 Dynamic
1   default   00-01-02-03-04-00  CPU  Self
1   default   00-01-02-03-04-05  1:10 Dynamic
1   default   00-01-30-10-2C-C7  1:10 Dynamic
1   default   00-01-30-FA-5F-00  1:10 Dynamic
1   default   00-02-3F-63-DD-68  1:10 Dynamic
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

config multicast port_filtering_mode

目的

指定したポートにマルチキャストパケットフィルタリングモードを設定します。

構文

config multicast port_filtering_mode [<portlist>|all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]

説明

指定したポート のためにスイッチにマルチキャストパケットフィルタリングモードを設定します。

パラメータ

パラメータ	説明
<portlist> | all	• <portlist> - 設定を行う port を指定します。 • all - 規則はすべての VLAN に適用されます。
forward_all_groups | forward_unregistered_groups | filter_unregistered_groups	これらの 3 つのオプションのいずれにもフィルタリングモードを設定することができます。 • forward_all_groups - すべてのグループを送信します。 • forward_unregistered_groups - 未登録のグループを送信します。 • filter_unregistered_groups - 未登録のグループをフィルタします。

制限事項

管理者レベルのみ本コマンドを実行できます。

使用例

ポートにマルチキャストフィルタリングモードを設定します。

```
DES-3526:admin#config multicast port_filtering_mode 15:1-15:4 forward_all_groups
Command: config multicast port_filtering_mode 15:1-15:4 forward_all_groups
Success.
DES-3526:admin#
```

show multicast port_filtering_mode

目的

ポート に設定されているマルチキャストパケットフィルタリングモードを表示します。

構文

show multicast port_filtering_mode {<portlist>}

説明

指定したポートまたはすべてのポート に対するスイッチの現在のマルチキャストパケットフィルタリングモードを表示します。

パラメータ

パラメータ	説明
<ipaddr>	マルチキャストフィルタリングステータスを表示します。

制限事項

なし。

使用例

ポート に対するスイッチの現在のマルチキャストパケットフィルタリングモードを表示します。

```
DES-3526:admin#show multicast port_filtering_mode
Command: show multicast port_filtering_mode
Port Multicase Filter Mode
------ --------------------------
1 forward_all_groups
2 forward_all_groups
3 forward_all_groups
4 forward_all_groups
5 forward_unregistered_groups
6 forward_unregistered_groups
7 forward_unregistered_groups
8 forward_unregistered_groups
9 forward_unregistered_groups
10 forward_unregistered_groups
11 filter_unregistered_groups
12 filter_unregistered_groups
DES-3526:admin#
```

第 12 章　トラフィックコントロールコマンド

コンピュータネットワーク上にはマルチキャストパケットやブロードキャストパケットなどのパケットが正常な状態でも絶えずあふれています。このトラフィックはネットワーク上の端末の不良や、故障したネットワークカードなどのように誤動作しているデバイスによって増加することもあります。そのため、スイッチのスループットに関する問題が発生し、その結果、ネットワークの全体的なパフォーマンスにも影響する可能性があります。このパケットストームを調整するために、本スイッチは状況を監視し、制御します。
パケットストームを監視し、ユーザが指定したしきい値を基にパケットがネットワークにあふれているどうか判断します。パケットストームが検出されると本スイッチはパケットストームが緩和されるまで受信したパケットを破棄します。この方法を使用するためには、「action」フィールドの「Drop」オプションを設定します。スイッチのチップカウンタを監視することによりスイッチに入力するパケットのスキャンとモニタを行います。チップにはブロードキャストとマルチキャストパケット用のカウンタのみ存在するため、この方法はブロードキャストストームとマルチキャストストームに対してのみ有効です。ストームが検出されると（以下で設定するパケット数のしきい値を超過すると）、スイッチは STP BPDU パケットを除くすべてのトラフィックの入力に対して、「countdown」フィールドで指定した時間、ポートをシャットダウンします。本時間経過後もパケットストームが続くようであれば、そのポートは「Shutdown Forever」（永久シャットダウン）モードに遷移し、トラップレシーバに送信する警告メッセージを生成します。一度「Shutdown Forever」モードに入ると、本ポートを通常の状態に戻すには、無効になっているポートを手動で有効状態に戻すしか方法はありません。このようなストームコントロール機能を利用するためには、「action」フィールドで「shutdown」オプションを選択してください。
コマンドラインインタフェース（CLI）におけるブロードキャストストームコントロールコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config traffic control	[<storm_grouplist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | time_interval <sec 5-30> | countdown [0 | <minute 5-30>]}
show traffic control	show traffic control {[group_list <storm_grouplist> | port <portlist>]}
config traffic trap	[none | storm_occurred | storm_cleared | both]

次のセクションで各コマンドについて詳しく説明します。

config traffic control

目的

ブロードキャスト / マルチキャスト / dlf トラフィックコントロールを設定します。

構文

config traffic control [<storm_grouplist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | time_interval <sec 5-30> | countdown [0 | <minute 5-30>]}

説明

トラフィックコントロールを設定します。

パラメータ

パラメータ	説明
<storm_grouplist>	<storm_grouplist> - grouplist に指定するグループ番号と、それぞれのグループ番号に属するポートを示します。 • Group 1 - ポート 1-8 • Group 2 - ポート 9-16 • Group 3 - ポート 17-24 • Group 4 - ポート 9-16（DES-3550）、ギガビットポート 25（DES-3526） • Group 5 - ポート 33-40（DES-3550）、ギガビットポート 26（DES-3526） • Group 6 - ポート 41-48（DES-3550 のみ） • Group 7 - ギガビットポート 49（DES-3550 のみ） • Group 8 - ギガビットポート 50（DES-3550 のみ • all - すべてのポートにトラフィックコントロールを設定します。
broadcast [enable | disable]	ブロードキャストストームコントロールを「enable」（有効）または「disable」（無効）にします。
multicast [enable | disable]	マルチキャストストームコントロールを「enable」（有効）または「disable」（無効）にします。
Unicast [enable | disable]	トラフィックコントロールを「enable」（有効）または「disable」（無効）にします。
action [drop | shutdown]	トラフィックコントロールがスイッチに検出された場合に行うアクションを設定します。2 つのタイプを選択できます。 • drop - スイッチのハードウェアによるトラフィックコントロールを行います。選択すると、スイッチのハードウェアが指定したしきい値に基づくパケットストームの検知を行い、パケットストームが発生すると、状態が改善するまでパケットの廃棄を行います。 • shutdown - スイッチのソフトウェアによるトラフィックコントロールにより、トラフィックストームの発生を検知します。ストームが検出されると、スイッチはスパニングツリーの保持に必要である STP BPDU パケットを除くすべてのトラフィックの入力に対して、ポートをシャットダウンします。カウントタイマ経過後もパケットストームが続くようであれば、そのポートは「Shutdown Forever」（永久シャットダウン）モードに遷移します。一度「Shutdown Forever」モードに入ると、「config ports」コマンドを使用して無効になっているポートを手動で有効状態に戻すまで、使用することはできません。本オプションを選択する際は、スイッチのチップからパケットカウントを受け取ってパケットストームの発生を検知するために必要な「time_interval」の設定も必要となります。
threshold <value 0-255000>	指定されたトラフィックコントロールが起動するしきい値の上限。<value> は、ストームトラフィックコントロール測定のトリガーとなるスイッチが受信するブロードキャスト / マルチキャスト /dlf（pps）の値です。初期値は 131072 です。
time_interval <value 5-30>	スイッチのチップからトラフィックコントロール機能に送信する、マルチキャスト・ブロードキャストパケットカウントの送信間隔。このパケットカウントにより、いつ入力パケットがしきい値を超過したかを検出します。 • sec 5-30 - 値の範囲は 5-30 で、初期値は 5（秒）です。
countdown <value 0> <value 5-30>	本値は、スイッチがトラフィックストーム発生中のポートをシャットダウンするまでに待機する時間（分）を表します。本パラメータは、「action」フィールドで「shutdown」を指定し、ハードウェアによるトラフィックコントロールを行わない場合に有効です。 • <value 0> - ポートはシャットダウンされることはありません。（初期値） • <value 5-30> - シャットダウンするまでにスイッチが待機する時間（分）を 5-30 で指定します。「countdown」タイマ経過後もパケットストームが続くようであれば、そのポートは「Shutdown Forever」（永久シャットダウン）モードに遷移し、前述の「config ports」コマンドを使用して無効になっているポートを手動で有効状態に戻すまで使用することはできません。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

トラフィックコントロールを設定し、ブロードキャストストームコントロールシステムを有効にします。

```
DES-3526:admin#config traffic control all broadcast enable
Command: config traffic control all broadcast enable

Success.

DES-3526:admin#
```

config traffic control_trap

目的

トラフィックコントロールにトラップを設定します。

構文

config traffic control_trap [none | storm_occurred | storm_cleared | both]

説明

トラフィックストームトラップメッセージを設定します。

パラメータ

パラメータ	説明
none	トラフィックコントロールメカニズムの動作に関わらず、ストームトラップメッセージを送信しません。
storm occurred	ストームトラップ発生時にストームトラップメッセージを送信します。
storm cleared	スイッチがストームトラップを消失させた場合、ストームトラップメッセージを送信します。
both	ストームトラップ発生時と消失時にストームトラップメッセージを送信します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

トラフィックコントロールを設定し、ブロードキャストトラフィックコントロールを有効にします。

```
DES-3526:admin#config traffic trap storm_occurred
Command: config traffic trap storm_occurred

Success.

DES-3526:admin#
```

show traffic control

目的

トラフィックコントロール設定を表示します。

構文

show traffic control {[group_list <storm_grouplist> | port <portlist>]}

説明

スイッチの現在のトラフィックコントロール設定を表示します。

パラメータ

パラメータ	説明
group_list <storm_grouplist>	<storm_grouplist> - grouplist に表示するグループ番号と、それぞれのグループ番号に属するポートを示します。 • Group 1 - ポート 1-8 • Group 2 - ポート 9-16 • Group 3 - ポート 17-24 • Group 4 - ポート 9-16（DES-3550）、ギガビットポート 25（DES-3526） • Group 5 - ポート 33-40（DES-3550）、ギガビットポート 26（DES-3526） • Group 6 - ポート 41-48（DES-3550 のみ） • Group 7 - ギガビットポート 49（DES-3550 のみ） • Group 8 - ギガビットポート 50（DES-3550 のみ）
port<portlist>	表示するポートまたはポート範囲を指定します。指定しないと、すべてのポートを表示します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

なし。

使用例

トラフィックコントロール設定を表示します。

```
DES-3526:admin#show traffic control
Command: show traffic control

Traffic Storm Control Trap :[None]

Port Thres   Broadcast  Multicast  DLF      Action  Count Time       Shutdown
     hold    Storm      Storm      Storm            down  Interval   Forever
---- -----   --------   ---------- --------  ----   ----- --------   --------
1:1  131072  Enabled    Disabled   Disabled  drop     0       5
1:2  131072  Enabled    Disabled   Disabled  drop     0       5
1:3  131072  Enabled    Disabled   Disabled  drop     0       5
2:4  131072  Disabled   Disabled   Disabled  drop     0       5
1:5  131072  Disabled   Disabled   Disabled  drop     0       5
1:6  131072  Disabled   Disabled   Disabled  drop     0       5
1:7  131072  Disabled   Disabled   Disabled  drop     0       5
1:8  131072  Disabled   Disabled   Disabled  drop     0       5
1:9  131072  Disabled   Disabled   Disabled  drop     0       5
1:10 131072  Disabled   Disabled   Disabled  drop     0       5
1:11 131072  Disabled   Disabled   Disabled  drop     0       5
1:12 131072  Disabled   Disabled   Disabled  drop     0       5
1:13 131072  Disabled   Disabled   Disabled  drop     0       5
1:14 131072  Disabled   Disabled   Disabled  drop     0       5
1:15 131072  Disabled   Disabled   Disabled  drop     0       5
1:16 131072  Disabled   Disabled   Disabled  drop     0       5

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

第 13 章　QoS コマンド

本スイッチシリーズは、802.1p キューイング QoS（Quality of Service）をサポートしています。スイッチには、4 個のプライオリティキューがあり、その 1 つは、内部であって設定することはできません。プライオリティキューには、最高レベルの 3 番キュー（クラス 3）から最低レベルの 0 番キュー（クラス 0）までがあります。IEEE 802.1p（p0 から p7）に規定される 8 つのプライオリティタグはスイッチのプライオリティタグと以下のように関連付けされます。

- プライオリティ 0 は、スイッチの Q1 キューに割り当てられます。
- プライオリティ 1 は、スイッチの Q0 キューに割り当てられます。
- プライオリティ 2 は、スイッチの Q0 キューに割り当てられます。
- プライオリティ 3 は、スイッチの Q1 キューに割り当てられます。
- プライオリティ 4 は、スイッチの Q2 キューに割り当てられます。
- プライオリティ 5 は、スイッチの Q2 キューに割り当てられます。
- プライオリティ 6 は、スイッチの Q3 キューに割り当てられます。
- プライオリティ 7 は、スイッチの Q3 キューに割り当てられます。

プライオリティベースのスケジューリングでは、上位の優先度キューから処理します。本スイッチは、最も高いプライオリティキュー 3 から最も低いプライオリティキュー 0 までの 4 つのハードウェアプライオリティキューを持っています。各ハードウェアキューは、次に低いプライオリティがパケット送信を許可するまで、バッファにすべてのパケットを送信します。最も低いハードウェアプライオリティキューがすべてのパケットの転送を完了すると、最も高いハードウェアプライオリティキューは、受信しているすべてのパケットの送信を開始します。

コマンドラインインタフェース（CLI）における QoS コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config bandwidth_control	[<portlist>] {rx_rate [no_limit | <value 1-1000>] | tx_rate [no_limit <value 1-1000>]}
show bandwidth_control	<portlist>
config scheduling	<class_id 0-3> {max_packet <value 0-255> | max_latency <value 0-255>}
show scheduling	
config 802.1p user_priority	<priority 0-7> <class_id 0-3>
show 802.1p user_priority	
config 802.1p default_priority	[<portlist> | all] <priority 0-7>
show 802.1p default_priority	<portlist>

以下のセクションで各コマンドについて詳しく説明します。

config bandwidth_control

目的

ポートベースで帯域幅制御を設定します。

構文

config bandwidth_control [<portlist>] {rx_rate [no_limit | <value 1-1000>] | tx_rate [no_limit <value 1-1000>]}

説明

ポートベースで帯域幅制御を設定します。

パラメータ

パラメータ	説明
<portlist>	• <portlist> - 表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）
rx_rate [no_limit | <value 1-1000>	以下のパラメータは、上で指定したポートにおいてパケットの受信が可能な速度を指定します。 • no_limit - 指定ポートが受信するパケットの速度を制限しません。 • <value 1-1000> - 上記ポートで受信するパケット制限（Kbps）を指定します。
tx_rate [no_limit | <value 1-1000>	以下のパラメータは、上で指定したポートにおいてパケットの送信が可能な速度を指定します。 • no_limit - 指定ポートが送信するパケットの速度を制限しません。 • <value 1-1000> - 上記ポートで送信するパケット制限（Kbps）を指定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

帯域幅制御を設定します。

```
DES-3526:admin#config bandwidth_control 1 rx_rate 64 tx_rate 64
Command: config bandwidth_control 1 rx_rate 64 tx_rate 64

Success.

DES-3526:admin#
```

show bandwidth_control

目的

帯域幅制御テーブルを表示します。

構文

show bandwidth_control {<portlist>}

説明

スイッチの現在の帯域幅制御設定をポートベースで表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

なし。

使用例

帯域幅制御設定を表示します。

```
DES-3526:admin#show bandwidth_control 1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

Port    RX Rate       TX Rate       Effective RX        Effective TX
        (Mbit/sec)    (Mbit/sec)    (Mbit/sec)          (Mbit/sec)
------  ----------    ----------    ----------------    ----------------
1       no_limit      no_limit      no_limit            no_limit
2       no_limit      no_limit      no_limit            no_limit
3       no_limit      no_limit      no_limit            no_limit
4       no_limit      no_limit      no_limit            no_limit
5       no_limit      no_limit      no_limit            no_limit
6       no_limit      no_limit      no_limit            no_limit
7       no_limit      no_limit      no_limit            no_limit
8       no_limit      no_limit      no_limit            no_limit
9       no_limit      no_limit      no_limit            no_limit
10      no_limit      no_limit      no_limit            no_limit

DES-3526:admin#
```

config scheduling

目的

各 CoS キューにトラフィック・スケジューリングメカニズムを設定します。

構文

config scheduling <class_id 0-3> [max_packet <value 0-255> | max_latency <value 0-255>]

説明

スイッチには、4 個のプライオリティキューがあります。これら 4 つのキューの 1 つに入力パケットをマップする必要があります。本コマンドは、これらの 4 つのハードウェアプライオリティキューが空にされている順番を指定します。

スイッチの初期値（「config scheduling」コマンドが使用されない場合、または、または「config scheduling」コマンドが「max_packet」に 0 指定して入力された場合）では、最も高いプライオリティキュー（ハードウェアキュー 3）から最も低いプライオリティキュー（ハードウェアキュー 0）まで順番にハードウェアプライオリティキューを空にしていきます。各ハードウェアキューは、次に低いプライオリティがパケット送信を許可するまで、バッファにすべてのパケットを送信します。最も低いハードウェアプライオリティキューがすべてのパケットの転送を完了すると、最も高いハードウェアプライオリティキューはすべての受信パケットを再度転送します。

max_packet パラメータには、優先順位が次のキューがパケット送信を行う前に送信される、付与されたハードウェアプライオリティキューのパケットの最大数を指定します。例えば、3 の値が指定されると、最も高いハードウェアプライオリティキュー（No.3）は 3 つのパケットを送信可能で、その次に低いハードウェアプラオリティキュー (No.2) が 3 つのパケットなどを送信できます。これはキューのすべてが 3 つのパケットを送信するまで、継続します。さらに処理は繰り返されます。<value 0-255> に 0 を入力すると、max_packet はパケットの送信のためにコンビネーションキューを作成します。コンビネーションキューはサービスクラスによる Strict や Weight-Fair (WRR) による処理スケジュールをあわせて使用することができます。Max Packet が 0 のプライオリティサービスクラスは Strict プライオリティスケジューリングでパケットを転送します。Max Packet が 0 でない残りのサービスクラスは、Max Packet が 0 のプライオリティサービスクラスのパケットが空である間は重み付けされたラウンドロビン（WRR）でパケットを転送します。Max Packet が 0 のプライオリティサービスクラスがパケットを受け取るとこのサービスクラスは自動的に空になるまでパケットの転送を開始します。Max Packet が 0 のプライオリティサービスクラスが一度空になると、残りのプライオリティサービスクラスはパケット転送の重み付けされたラウンドロビン（WRR）のサイクルをいったんリセットし、最も高いプライオリティサービスクラスの処理を開始します。同レベルのプライオリティで Max Packet も等しいプライオリティサービスクラスの処理はハードウェアプライオリティスケジューリングに依存します。

パラメータ

パラメータ	説明
<class_id 0-3>	「config scheduling」コマンドが 4 つのハードウェアプライオリティキューのどれに適用されるかを指定します。4 つのハードウェアプライオリティキューは、最も低い優先度である 0 キューを持つ 0 から 3 の番号によって識別されます。
max_packet <value 0-255>	優先順位が次のキューがパケット送信を行う前に送信される、上で指定したハードウェアプライオリティキューのパケットの最大数を指定します。0 から 255 の間の値を指定します。
max_latency <value 0-255>	優先順位の次のキューからパケット送信を行う前に、指定したハードウェアプライオリティキューからパケット送信を行う最大時間を算出するための値です。0-255 で指定します。本値に 16ms を乗じた時間、そのキューからのパケット送信が許可されます。例えば 3 を指定すると、3 x 16 = 48 ms となります。本時間が満了するまでパケットの送信が行われます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

各キューにトラフィック・スケジューリングメカニズムを設定します。

```
DES-3526:admin#config scheduling 0 max_packet 12
Command: config scheduling 0 max_packet 12

Success.

DES-3526:admin#
```

show scheduling

目的

スイッチに設定されている現在のトラフィック・スケジューリングを表示します。

構文

show scheduling

説明

スイッチに使用中の現在のトラフィックスケジューリングメカニズムを表示します。

パラメータ

なし。

制限事項

なし。

使用例

現在のトラフィックスケジューリングメカニズムを表示します。

```
DES-3526:admin#show scheduling
Command: show scheduling

QOS Output Scheduling

        MAX. Packets
        -------------
Class-0          12
Class-1          2
Class-2          3
Class-3          4
Class-4          5
Class-5          6
Class-6          7
Class-7          8
```

config 802.1p user_priority

目的

スイッチで利用可能な 8 つのハードウェアキューの 1 つに入力パケットの 802.1p ユーザプライオリティをマップします。

構文

config 802.1p user_priority <priority 0-7> <class_id 0-3>

説明

802.1p ユーザプライオリティに基づいて、入力パケットを 4 つの有効なハードウェアプライオリティキューの 1 つにマップする方法を設定します。スイッチの初期状態では、今の通り入力する 802.1p ユーザプライオリティの値を 4 つのハードウェアプライオリティキューにマップします。

802.1p	ハードウェアキュー	備考
0	1	Mid-low
1	0	Lowest
2	0	Lowest
3	1	Mid-low
4	2	Mid-high
5	2	Mid-high
6	3	Highest
7	3	Highest

このマッピング体系は、IEEE 802.1D に含まれる勧告に基づいています。

このマッピングは、<class_id 0-3>（ハードウェアキューの番号）に対して 802.1p ユーザプライオリティを指定することで変更できます。

パラメータ

パラメータ	説明
<priority 0-7>	<class_id 0-3>（ハードウェアキューの番号）に連携させる 802.1p ユーザプライオリティ。
<class_id 0-3>	スイッチのハードウェアプライオリティキューの番号。本スイッチには、4 個のプライオリティキューがあります。それらは 0（最も低いプライオリティ）と 3（最も高いプライオリティ）の間で番号を付与されます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチに 802.1p ユーザプライオリティを設定します。

```
DES-3526:admin#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DES-3526:admin#
```

show 802.1p user_priority

目的

入力パケットの 802.1p ユーザプライオリティ値とスイッチの 4 つのハードウェアプライオリティキューとの現在のマッピングを表示します。

構文

show 802.1p user_priority

説明

入力パケットの 802.1p ユーザプライオリティ値とスイッチの 4 つのハードウェアプライオリティキューとの現在のマッピングを表示します。

パラメータ

なし。

制限事項

なし。

使用例

802.1p ユーザプライオリティを表示します。

```
DES-3526:admin#show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

Priority-0  ->  <Class-2>
Priority-1  ->  <Class-3>
Priority-2  ->  <Class-1>
Priority-3  ->  <Class-3>
Priority-4  ->  <Class-0>
Priority-5  ->  <Class-2>
Priority-6  ->  <Class-3>
Priority-7  ->  <Class-2>

DES-3526:admin#
```

config 802.1p default_priority

目的

スイッチの 802.1p デフォルトプライオリティ設定を指定します。タグなしパケットをスイッチが受信すると、本コマンドで設定したプライオリティは、パケットのプライオリティフィールドに記載されます。

構文

config 802.1p default_priority [<portlist> | all] <priority 0-7>

説明

スイッチが受信したタグなしパケットのデフォルトプライオリティ処理に関する指定をします。本コマンドで入力されたプライオリティ値は、パケットが 7 つのハードウェアプライオリティキューのうちのどれに送信されるかを決定するために使用されます。

パラメータ

パラメータ	説明
<portlist> | all	• <portlist> - 表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - スイッチのすべてのポートに適用します。
<priority 0-7>	スイッチまたはスイッチのポート範囲が受信したタグなしパケットに割り当てるプライオリティ値。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチに 802.1p デフォルトプライオリティを設定します。

```
DES-3526:admin#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DES-3526:admin#
```

show 802.1p default_priority

目的

宛先に転送される前に入力するタグなしパケットに割り当てられている現在の 802.1p プライオリティ値を表示します。

構文

show 802.1p default_priority {<portlist>}

説明

宛先に転送される前に入力するタグなしパケットに割り当てられている現在の 802.1p プライオリティ値を表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

なし。

使用例

スイッチの現在の 802.1p デフォルトプライオリティ設定を表示します。

```
DES-3526:admin#show 802.1p default_priority
Command: show 802.1p default_priority

Port    Priority
------  --------
1       0
2       0
3       0
4       0
5       0
6       0
7       0
8       0
9       0
10      0
11      0
12      0
13      0
14      0
15      0
16      0
17      0
18      0
19      0
20      0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

第 14 章　ポートミラーリングコマンド

コマンドラインインタフェース（CLI）におけるポートミラーリングコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config mirror port	<port> [add | delete] source ports <portlist> [rx | tx | both]
enable mirror	
disable mirror	
show mirror	

以下のセクションで各コマンドについて詳しく記述します。

config mirror port

目的

スイッチにミラーポートとソースポートのペアを設定します。どのソースポートからターゲットポートまでのトラフィックもリアルタイム分析のためにミラーリングできます。ロジックアナライザや RMON プローブを接続し、ソースポートを通過するトラフィックを調べることができます。

構文

config mirror port <port> [add | delete] source ports <portlist> [rx | tx | both]

説明

ポート範囲は、代表ポートに送信されるすべてのトラフィックを持つことが可能で、ネットワークスニファーや他のデバイスがネットワークトラフィックをモニタすることができます。さらに、1 方向または両方向に送受信されるトラフィックだけがターゲットポートにミラーリングされるような指定も可能です。

パラメータ

パラメータ	説明
<port>	ミラーされたパケットを受信するターゲットポートを指定します。ターゲットポートは、ソースポートと同じ VLAN に設定され、ソースポートと同じ速度で動作する必要があります。ターゲットポートがより低速で動作していると、ソースポートは、ターゲットポートに一致するように動作速度を落とします。ポートリストは、「:」（コロン）で分けられて、スイッチで最も下位のスイッチ番号と開始番号の一覧で指定されます。例えば、1:3 はスイッチ番号 1 のポート 3 を表しています。2:4 はスイッチ番号 2 のポート 4 を表しています。
add | delete	ソースポートパラメータに設定されるミラーポートの追加または削除をします。
source ports	ミラーされるポート（範囲）を指定します。これにはターゲットポートを含むことはできません。
rx | tx | both	• rx - ポートまたはポートリスト内のポートが受信するパケットだけをミラーリングします。 • tx - ポートまたはポートリスト内のポートが送信するパケットだけをミラーリングします。 • both - ポートまたはポートリスト内のポートが送受信するすべてのパケットをミラーリングします。

制限事項

ターゲットポートはソースポートにはできません。管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

```
DES-3526:admin#config mirror port 1 add source ports 2-7 both
Command: config mirror port 1 add source ports 2-7 both

Success.

DES-3526:admin#
```

ミラーリングポートを削除します。

```
DES-3526:admin#config mirror port 1:1 delete source ports 2-7 both
Command: config mirror port 1:1 delete source ports 2-7 both

Success.

DES-3526:admin#
```

enable mirror

目的
入力したポートミラーリング設定を有効にします。
構文
enable mirror
説明
スイッチにポートミラーリング設定を入力した後に、設定を変更しないでミラーリングを有効にします。
パラメータ
なし。
制限事項
管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。
使用例
ミラーリング設定を有効にします。

```
DES-3526:admin#enable mirror
Command: enable mirror

Success.

DES-3526:admin#
```

disable mirror

目的
設定したポートミラーリング設定を無効にします。
構文
disable mirror
説明
スイッチにポートミラーリング設定を入力した後に、設定を変更しないでミラーリングを無効にします。
パラメータ
なし。
制限事項
管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。
使用例
ミラーリング設定を無効にします。

```
DES-3526:admin#disable mirror
Command: disable mirror

Success.

DES-3526:admin#
```

show mirror

目的

スイッチの現在のポートミラーリング設定を表示します。

構文

show mirror

説明

スイッチの現在のポートミラーリング設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

ミラーリング設定を表示します。

```
DES-3526:admin#show mirror
Command: show mirror

Current Settings
Mirror Status :Enabled
Target Port   :1:1
Mirrored Port
           RX :
           TX :1:5-1:7

DES-3526:admin#
```

第 15 章　VLAN コマンド

本スイッチは、通常の VLAN 設定はもちろんダブル VLAN もサポートしています。ダブル VLAN または Q-in-QDES-3526:admin#VLAN と呼ばれる技術を利用することにより、ネットワークプロバイダは規模の大きい包括的な VLAN の中に、顧客用の VLAN を設置し、VLAN 構成に新しい階層を導入することで可能となり、その規模を拡張することができます。基本的には大規模な ISP のネットワーク内に、レイヤ 2 の VPN（Virtual Private Network）および、顧客用の透過型 LAN を配置することにより、クライアント側の構造を複雑にすることなく、複数の顧客の LAN を接続します。構造の複雑化が回避できるだけでなく、4000 以上の VLAN を定義できるようになるため、VLAN ネットワークを大幅に拡張することができます。

本機能は ISP VLAN 認識と分類のために既存の VLAN フレームに VLAN フレームを追加します。デバイス通知を確実にするため、tpid として知られているこの追加 VLAN フレーム（イーサネットカプセル化）が、さらにフレームに追加されます。デバイスは、この tpid を認識して、プロバイダ VLAN タグが追加されたかどうかを確認するために VLAN のタグ付きパケットをチェックします。その場合、パケットの宛先への迅速で信頼性の高いルーティングを保証するために、同様の設定を持つさらに小規模の VLAN を含むこのプロバイダ VLAN を経由してパケットは送信されます。

コマンドラインインタフェース（CLI）における VLAN コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create vlan	<vlan_name 32> {tag <vlanid 1-4094> | advertisement}
delete vlan	<vlan_name 32>
config vlan	<vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}
config gvrp	[<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}
enable gvrp	
disable gvrp	
show vlan	{<vlan_name 32>}
show gvrp	{<vlan_name 32>}

次のセクションで各コマンドについて詳しく説明します。

create vlan

目的

スイッチに VLAN を作成します。

構文

create vlan <vlan_name 32> {tag <vlanid 1-4094> | advertisement}

説明

スイッチに VLAN を作成します。802.1Q VLAN またはプロトコルベース VLAN を選択します。

パラメータ

パラメータ	説明
<vlan_name 32>	作成する VLAN 名。
tag <vlanid 1-4094>	作成する VLAN の VLAN ID。1-4094 で指定します。
advertisement	LAN が GVRP に連携するように指定します。本パラメータが設定されないと、スイッチは VLAN に関するすべての GVRP メッセージを送信することができません。

制限事項

各 VLAN 名は 32 文字以内で指定します。管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

VLAN「v1」、「tag2」を作成します。

```
DES-3526:admin#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DES-3526:admin#
```

delete vlan

目的

スイッチに設定済みの VLAN を削除します。

構文

delete vlan <vlan_name 32>

説明

スイッチに設定済みの VLAN を削除します。

パラメータ

パラメータ	説明
<vlan_name 32>	削除する VLAN 名。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

VLAN「v1」を削除します。

```
DES-3526:admin#delete vlan v1
Command: delete vlan v1

Success.
```

config vlan

目的

設定済みの VLAN にポートを追加します。

構文

config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}

パラメータ

パラメータ	説明
<vlan_name 32>	ポートを追加する VLAN 名。
add	VLAN にポートを追加します。追加するポートには 3 つのタイプがあります。 • tagged - 追加ポートをタグ付きとします。 • untagged - 追加ポートをタグなしとします。 • forbidden - 追加ポートを禁止ポートにします。
delete	指定した VLAN からポートを削除します。
<portlist>	指定した VLAN に追加するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）
advertisement [enable | disable]	指定 VLAN 上の GVRP を「enable」（有効）または「disable」（無効）にします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

VLAN v1 にタグ付きポート（ポート 1-8）を追加します。

```
DES-3526:admin#config vlan v1 add tagged 1:4-1:8
Command: config vlan v1 add tagged 1:4-1:8

Success.

DES-3526:admin#
```

config gvrp

目的

スイッチに GVRP を設定します。

構文

config gvrp [<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}

説明

スイッチに GVRP を設定します。イングレスチェック、GVRP 情報の送受信、およびポート VLAN ID（PVID）を設定します。

パラメータ

パラメータ	説明
<portlist>	• <portlist> - GVRP を有効にするポートまたは範囲を指定しますポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - スイッチのすべてのポートを指定します。
state [enable | disable]	ポートリストに指定されたポートに GVRP 機能を「enable」（有効）または「disable」（無効）にします。
ingress_checking [enable | disable]	指定ポートに対するイングレスチェックを「enable」（有効）または「disable」（無効）にします。
acceptable_frame [tagged_only | admit_all]	本機能のためにスイッチが受け入れるフレームタイプを示します。 • tagged_only - タグ付きの VLAN フレームだけを受け入れることを示します。 • admit_all - タグ付きおよびタグなしフレームを受け入れることを示します。
pvid <vlanid 1-4094>	ポートに関連するデフォルト VLAN ID を指定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

イングレスチェック状態、GVRP 情報の送受信を設定します。

```
DES-3526:admin#config gvrp 1:1-1:4 state enable ingress_checking enable acceptable_frame tagged_only
pvid 2
Command: config gvrp 1:1-1:4 state enable ingress_checking enable acceptable_frame tagged_only pvid 2

Success.

DES-3526:admin#
```

注意 現在のファームウェアバージョンでは、これらのポートをタグなしメンバとして VLAN に追加する場合、ポートへの PVID は、手動設定、または自動割り当てによって設定します。

enable gvrp

目的

スイッチの GVRP を有効にします。

構文

enable gvrp

説明

スイッチの GVRP 設定を変更しないで、スイッチの GVRP を有効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

GVRP を有効にします。

```
DES-3526:admin#enable gvrp
Command: enable gvrp

Success.

DES-3526:admin#
```

disable gvrp

目的

スイッチの GVRP を無効にします。

構文

disable gvrp

説明

スイッチの GVRP 設定を変更しないで、スイッチの GVRP を無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

GVRP を無効にします。

```
DES-3526:admin#disable gvrp
Command: disable gvrp

Success.

DES-3526:admin#
```

show vlan

目的

スイッチの現在の VLAN 設定を表示します。

構文

show vlan {[<vlan_name 32> | port <port>]}

説明

VLAN ID、VLAN 名、タグ付き / タグなしステータス、および VLAN のメンバである各ポートの Member/Non-member/Forbidden ステータスを含む各 VLAN に関するサマリ情報を表示します。

パラメータ

パラメータ	説明
<vlan_name 32>	サマリ設定を表示する VLAN 名。
port <port>]}	サマリ設定を表示するポート名。

制限事項

なし。

使用例

スイッチの現在の VLAN 設定を表示します。

```
DES-3526:admin#show vlan
Command: show vlan

VID                   : 1                   VLAN Name       : default
VLAN Type             : Static              Advertisement   : Enabled
Member ports          : 1-12
Static ports          : 1-12
Current Tagged Ports  :
Current Untagged Ports : 1-12
Static Tagged Ports   :
Static Untagged Ports  : 1-12
Forbidden Ports:

Total Entries : 1

DES-3526:admin#
```

show gvrp

目的

スイッチのポートリストに対する GVRP ステータスを表示します。

構文

show gvrp {<portlist>}

説明

スイッチのポートリストに対する現在の GVRP ステータスを表示します。

パラメータ

パラメータ	説明
<portlist>	GVRP ステータスを表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

なし。

使用例

GVRP ポートステータスを表示します。

```
DES-3526:admin#show gvrp
Command: show gvrp

Global GVRP :Disabled

Port PVID GVRP     Ingress Checking Acceptable Frame Type
---- ---- -------- ---------------- --------------------
1:1  1    Disabled Enabled           All Frames
1:2  1    Disabled Enabled           All Frames
1:3  1    Disabled Enabled           All Frames
1:4  1    Disabled Enabled           All Frames
1:5  1    Disabled Enabled           All Frames
1:6  1    Disabled Enabled           All Frames
1:7  1    Disabled Enabled           All Frames
1:8  1    Disabled Enabled           All Frames
1:9  1    Disabled Enabled           All Frames
```

第 16 章　Asymmetric VLAN コマンド

コマンドラインインタフェース（CLI）における Asymmetric VLAN コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable asymmetric_vlan	
disable asymmetric_vlan	
show asymmetric_vlan	

以下のセクションで各コマンドについて詳しく説明します。

enable asymmetric_vlan

目的

スイッチの Asymmetric VLAN 機能を有効にします。

構文

enable asymmetric_vlan

説明

スイッチの Asymmetric VLAN 機能を有効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

Asymmetric VLAN 機能を有効にします。

```
DES-3526:admin#enable asymmetric_vlan
Command: enable asymmetric_vlan
Success.
DES-3526:admin#
```

disable asymmetric_vlan

目的

スイッチの Asymmetric VLAN 機能を無効にします。

構文

enable asymmetric_vlan

説明

スイッチの Asymmetric VLAN 機能を無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

Asymmetric VLAN 機能を無効にします。

```
DES-3526:admin#disable asymmetric_vlan
Command: disable asymmetric_vlan
Success.
DES-3526:admin#
```

show asymmetric_vlan

目的

スイッチの Asymmetric VLAN 機能の設定を表示します。

構文

asymmetric_vlan

説明

スイッチの Asymmetric VLAN 機能の設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

Asymmetric VLAN 機能の設定を表示します。

```
DES-3526:admin#show asymmetric_vlan
Command: show asymmetric_vlan
Asymmetric VLAN: Enabled
DES-3526:admin#
```

第 17 章　リンクアグリゲーションコマンド

コマンドラインインタフェース（CLI）におけるリンクアグリゲーションコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create link_aggregation	group_id <value 1-6> {type [lacp | static]}
delete link_aggregation	group_id <value 1-6>
config link_aggregation	group_id <value 1-6> {master_port <port> | ports <portlist> | state [enable | disable]}
config link_aggregation	[mac_source | mac_destination | mac_source_dest | ip_source |
algorithm	ip_destination | ip_source_dest]
show link_aggregation	{group_id <value 1-6> | algorithm}
config lacp_port	<portlist> mode [active | passive]
show lacp_port	{<portlist>}

以下のセクションで各コマンドについて詳しく説明します。

create link_aggregation group_id

目的

固有の識別子を持つリンクアグリゲーショングループを作成します。

構文

create link_aggregation group_id <value 1-6> {type [lacp | static]}

説明

固有の識別子を持つリンクアグリゲーショングループを作成します。

パラメータ

パラメータ	説明
<value 1-6>	グループ ID を指定します。スイッチは、最大 6 個のリンクアグリゲーショングループを設定することが可能です。グループ番号は、各グループを識別します。
type	グループに使用されるリンクアグリゲーションのタイプを指定します。タイプが指定されないと、初期値は「static」になります。 • lacp - ポートグループを LACP 準拠として指定します。これにより LACP は集約されたポートグループに動的な変更を行います。（「config lacp_ports」コマンド参照。）LACP デバイス同士でないと通信できません。 • static - アグリゲーションポートグループをスタティックに指定します。トランクグループの設定が変更されると、リンクするデバイスの両方が手動で設定される必要があるため、スタティックポートグループは LACP 対応のポートグループと同様に容易に変更することはできません。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

リンクアグリゲーショングループを作成します。

```
DES-3526:admin#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DES-3526:admin#
```

delete link_aggregation group_id

目的

定義済みのリンクアグリゲーショングループを削除します。

構文

delete link_aggregation group_id <value 1-6>

説明

既存のリンクアグリゲーショングループを削除します。

パラメータ

パラメータ	説明
<value 1-6>	削除するグループ ID を指定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

リンクアグリゲーショングループを削除します。

```
DES-3526:admin#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

DES-3526:admin#
```

config link_aggregation group_id

目的

既存のリンクアグリゲーショングループを設定します。

構文

config link_aggregation group_id <value 1-6> {master_port <port> | ports <portlist> state [enable|disable]}

説明

既存のリンクアグリゲーショングループを設定します。

パラメータ

パラメータ	説明
master_port <port>	マスタポート番号。マスタポートになるリンクアグリゲーショングループのポート番号を指定します。リンクアグリゲーショングループのすべてのポートは、マスタポートと共にポート設定を共有します。ポートは、「:」（コロン）で分けることによって、最も下位のスイッチ番号と始めのポート番号によって指定されます。
ports <portlist>	リンクアグリゲーショングループに所属するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）
state [enable|disable]	指定されたリンクアグリゲーショングループを「enable」（有効）または「disable」（無効）にします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

リンクアグリゲーショングループは重複することはできません。

使用例

ポートの負荷分散グループ、グループ ID1、マスタポート 5 をグループメンバポート 5-7 およびポート 9 と共に定義します。

```
DES-3526:admin#config link_aggregation group_id 1 master_port 1:5 ports 1:5-
1:7,1:9
Command: config link_aggregation group_id 1 master_port 1:5 ports 1:5-1:7,1:9

Success.

DES-3526:admin#
```

config link_aggregation algorithm

目的

リンクアグリゲーションアルゴリズムを設定します。

構文

config link_aggregation algorithm [mac_source | mac_destination |mac_source_dest | ip_source | ip_destination | ip_source_dest]

説明

送信の負荷分散データに対してイーグレスポートを選択する場合、スイッチに検証されるパケットの部分を設定します。この機能は、アドレスベースの負荷分散アルゴリズムを使用することで有効になります。

パラメータ

パラメータ	説明
mac_source	スイッチは送信元 MAC アドレスを調べます。
mac_destination	スイッチは送信先 MAC アドレスを調べます。
mac_source_dest	スイッチは送信元および送信先 MAC アドレスを調べます。
ip_source	スイッチは送信元 IP アドレスを調べます。
ip_destination	スイッチは送信先 IP アドレスを調べます。
ip_source_dest	スイッチは送信元 IP アドレスを調べます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

mac-source-dest にリンクアグリゲーションアルゴリズムを設定します。

```
DES-3526:admin#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DES-3526:admin#
```

show link_aggregation

目的

スイッチの現在のリンクアグリゲーショングループを表示します。

構文

show link_aggregation {group_id <value 1-6> | algorithm}

説明

スイッチの現在のリンクアグリゲーショングループを表示します。

パラメータ

パラメータ	説明
<value 1-6>	グループ ID を指定します。スイッチは、最大 6 個のリンクアグリゲーショングループを設定することが可能です。グループ番号は、各グループを識別します。
algorithm	使用中のアルゴリズムで指定されるリンクアグリゲーションを表示します。

制限事項

なし。

使用例

リンクアグリゲーション設定を表示します。

```
DES-3526:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithem = MAC-source-dest
Group ID      :1
Type          :TRUNK
Master Port   :1:8
Member Port   :1:8-1:10
Active Port   :
Status        :Disabled
Flooding Port :8

Total Entries : 1

DES-3526:admin#
```

config lacp_port

目的

以前に LACP ポートとして指定されたポートを設定します。

構文

config lacp_port <portlist> mode [active | passive]

説明

以前に LACP ポートとして指定されたポートを設定します（「create link_aggregation」を参照）。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）
mode [active | passive]	LACP ポートが LACP 制御フレームを処理するかどうかを決定するモードを選択します。 • active - Active LACP ポートは、LACP 制御フレームの処理と送信を行います。これにより LACP 準拠のデバイス同士はネゴシエーションとリンクの集約を行い、グループは必要に応じて動的に変更されます。グループへのポート追加、または削除などのグループの変更を行うためには、少なくともどちらかのデバイスで LACP ポートを「Active」に設定する必要があります。また、両方のデバイスは LACP をサポートしなければなりません。 • passive - passive に設定された LACP ポートは、LACP 制御フレームの処理を行いません。リンクするポートグループがネゴシエーションを行い、動的にグループの変更を行うには、接続のどちらか一端が「active」LACP ポートである必要があります（上記参照）。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

LACP ポートモード設定を行います。

```
DES-3526:admin#config lacp_port 1:1-1:12 mode active
Command: config lacp_port 1:1-1:12 mode active

Success.

DES-3526:admin#
```

show lacp_port

目的

現在の LACP ポートモード設定を表示します。

構文

show lacp_port {<portlist>}

説明

現在の LACP ポートモード設定を表示します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。ポートリストは、「:」(コロン)で分け、スイッチ番号と開始番号の一覧で指定されます。 ポートの範囲は、「-」(ダッシュ)を使用して指定します。続き番号ではないポートリストエントリは「,」(カンマ)で分けます。 (例 : 1:1-1:3,1:7-1:9) パラメータが指定されないと、システムはすべてのポートの現在の LACP ステータスを表示します。

制限事項

なし。

使用例

LACP ポートモード設定を表示します。

```
DES-3526:admin#show lacp_port 1:1-1:10
Command: show lacp_port 1:1-1:10

Port Activity
---- ----------
1:1  Active
1:2  Active
1:3  Active
1:4  Active
1:5  Active
1:6  Active
1:7  Active
1:8  Active
1:9  Active
1:10 Active
```

第 18 章　IP-MAC-Port バインディング（IMPB）コマンド

ネットワーク構造においてネットワーク層（IP レベル）では 4 バイトの IP アドレス、データリンク層（データリンクレベル）では 6 バイトの MAC アドレスが使用されています。本機能ではこれらの 2 種類のアドレスタイプ (IP と MAC) を関連付けてデータ転送をすることができます。IP-MAC-Port バインディングの第一の目的は、スイッチにアクセスするユーザ数を制限することです。IP アドレスと MAC アドレスのペアを事前に設定したデータベースリストから照らし合わせて、リストに対応する認証クライアントのみがスイッチのポートにアクセスすることができます。未認証のクライアントが IP-MAC-Port バインディングが有効なポートにアクセスしようとしても、ブロックされパケットは廃棄されます。IP-MAC-Port バインディングのエントリ数はチップの能力（例えば ARP テーブルサイズ）およびデバイスのストレージサイズによって異なり、本シリーズにおける IP-MAC-Port バインディングの最大エントリ数は 512 です。認証クライアントのリストは、CLI または Web により作成することができます。本機能は各ポートごとに有効 / 無効にすることができます。

ACL モード

IP-MAC-Port バインディングで生じたいくつかの特別なケースのために、IP-MAC-Port バインディングに特別な ACL モードを実装しています。これは、これらの問題を軽減することができます。有効にすると、スイッチはアクセスプロファイルテーブルに 2 つのエントリを作成します。スイッチに利用可能なプロファイル番号が少なくとも 2 つある場合にだけ、エントリは作成されます。そうでない場合に ACL モードが有効にされると、エラーメッセージが表示されます。ACL モードが有効にされる場合、スイッチは IP-MAC-Port バインディング設定で作成されたエントリからのパケットだけを受信します。他のすべてのパケットは破棄されます。
ACL モードを設定するためには、はじめに「create address_binding ip_mac ipaddress」コマンドで IP-MAC-Port バインディングを作成し、ACL モードを選択する必要があります。その後、「enable address_binding acl_mode」コマンドを入力することでモードを有効にする必要があります。IP-MAC-Port バインディングエントリを作成し、それを ACL モードエントリに変更する場合には、「config address_binding ip_mac ipaddress」コマンドを使用して、ACL モードを選択します。

注意 IP-MAC-Port バインディング機能の ACL モードの設定を行う時は、登録済みの ACL エントリの内容に十分ご注意ください。ACL モードエントリは、若い空き番号から 2 つの ID を使用し、またアクセスプロファイル ID は、ACL プライオリティ（優先度）を示すため、ACL モードエントリが他の ACL エントリより優先されてしまう可能性があります。ACL エントリが優先されることにより設定内容の競合が発生し、ユーザ定義の ACL パラメータが無効になる恐れがあります。ACL 設定についての詳しい情報は、「24 章 アクセスコントロールリスト (ACL) コマンド」を参照してください。

注意 ACL プロファイルを IP-MAC-Port バインディング機能を通じて作成すると、それらの ACL モードアクセスプロファイルエントリに対して編集、削除または追加はできません。ACL ルールの編集、削除または追加を行うと前画面にエラーメッセージが表示されます。

注意 スイッチにコンフィグレーションファイルをアップロードする場合、ロードされる ACL 設定に注意してください。本機能によって設定された ACL モードのアクセスプロファイルは、アクセスプロファイルタイプの両方に問題を引き起こす可能性があります。

コマンドラインインタフェース（CLI）における IP-MAC-Port バインディングコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> | all] | mode {arp | acl]}
config address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> | all] | mode {arp | acl]}
config address_binding ip_mac ports	[<portlist> | all] state [enable | disable]
config address_binding ip_mac ports	[allow_zeroip [eable|disable]
show address_binding	[ip_mac {[all | ipaddress <ipaddr> mac_address <macaddr>]} | blocked {[all | vlan_name <vlan_name> mac_address <macaddr>]} | ports]
delete address_binding	[ip-mac [ipaddress <ipaddr> mac_address <macaddr> |all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]
enable address_binding acl_mode	
disable address_binding acl_mode	
enable address_binding trap_log	
disable address_binding trap_log	

create address_binding ip_mac ipaddress

目的

IP-MAC-Port バインディングエントリを作成します。

構文

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all] | mode [arp | acl]}

説明

IP-MAC-Port バインディングエントリを作成します。

パラメータ

パラメータ	説明
<ipaddr>	IP-MAC-Port バインディングが行われるデバイスの IP アドレス。
mac_address <macaddr>	IP-MAC-Port バインディングが行われるデバイスの MAC アドレス。
ports [<portlist> | all]	• <portlist> - アドレスバインディングを設定するポートまたはポート範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - スイッチのすべてのポートがアドレスバインディングに設定されます。
mode [arp | acl]	以下の 2 つのモードのいずれかを選択することによって、IP-MAC-Port バインディング設定のモードを設定します。 • arp - 入力した IP と MAC アドレスにより、通常の IP-MAC-Port バインディングエントリを設定します。 • acl - 送信元がここで作成した IP-MAC-Port バインディングエントリであるパケットだけを許可します。異なる IP アドレスを持つそれ以外のパケットは廃棄されます。本モードは、「enable address_binding acl_mode」コマンドで ACL モードを有効にした場合にだけ使用できます。

制限事項

管理者レベルユーザおよびオペレータレベルのみ本コマンドを実行できます。

使用例

スイッチのアドレスバインディングを作成します。

```
DES-3526:admin#create address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-
00-04
Command: create address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-04

Success.
DES-3526:admin#
```

ACL モードでスイッチのアドレスバインディングを作成します。

```
DES-3526:admin#create address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-04 mode
acl
Command: create address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-04 mode acl

Success.
DES-3526:admin#
```

config address_binding ip_mac ipaddress

目的

本コマンドは IP-MAC-Port バインディングエントリを設定します。

構文

config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all] | mode [arp | acl]}

説明

本コマンドは IP-MAC-Port バインディングエントリを設定します。

パラメータ

パラメータ	説明
<ipaddr>	IP-MAC-Port バインディングが行われるデバイスの IP アドレス。
<macaddr>	IP-MAC-Port バインディングが行われるデバイスの MAC アドレス。
ports [<portlist> | all]	• <portlist> - アドレスバインディングを設定するポートまたはポート範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - スイッチのすべてのポートがアドレスバインディングに設定されます。
mode [arp | acl]	以下の 2 つのモードのいずれかを選択することによって、IP-MAC-Port バインディング設定のモードを設定します。 • arp - 入力した IP と MAC アドレスにより、通常の IP-MAC-Port バインディングエントリを設定します。 • acl - 送信元がここで作成した IP-MAC-Port バインディングエントリであるパケットだけを許可します。異なる IP アドレスを持つそれ以外のパケットは廃棄されます。本モードは、「enable address_binding acl_mode」コマンドで ACL モードを有効にした場合にだけ使用できます。

制限事項

管理者レベルユーザおよびオペレータレベルのみ本コマンドを実行できます。

使用例

スイッチにアドレスバインディングを設定します。

```
DES-3526:admin#config address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-
00-05
Command: config address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-05

Success.

DES-3526:admin#
```

ACL モードでスイッチのアドレスバインディングを設定します。

```
DES-3526:admin#config address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-05 mode
acl
Command: config address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-05 mode acl

Success.

DES-3526:admin#
```

config address_binding ip_mac ports

目的

指定されたポートに対して IP-MAC 状態を有効または無効に設定します。

構文

config address_binding ip_mac ports [<portlist>| all] {state [enable {[strict | loose]} | disable] |allow_zeroip [enable | disable] |forward_dhcppkt [enable | disable]}

説明

指定されたポートに対して IP-MAC 状態を有効または無効に設定します。

パラメータ

パラメータ	説明
ports [<portlist> | all]	• <portlist> - 設定するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - スイッチのすべてのポートがアドレスバインディングに設定されます。
state[enable {[strict | loose]} | disable]	指定されたポートに対して IP-MAC 状態を「enable」（有効）または「disable」（無効）に設定します。 [strict | loose] - strict - アドレスバインディングに符合しない IP のパケットは排除します。 - loose - 符号しないパケットであっても通り抜けることはできます。（符合するパケットののみ有効と判断されます）
allow_zeroip [enable | disable]	• ゼロサブネットを「enable」（有効）または「disable」（無効）にします。
forward_dhcppkt [enable | disable]	• DHCP パケットの送信を「enable」（有効）または「disable」（無効）にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチにアドレスバインディングを設定します。

```
DES-3526:admin#config address_binding ip_mac ports 1:2 state enable
Command: config address_binding ip_mac ports 1:2 state enable

Success.

DES-3526:admin#
```

show address_binding

目的

IP-MAC-Port バインディングエントリを表示します。

構文

show address_binding [ip_mac {[all | ipaddress <ipaddr> mac_address <macaddr>]} | blocked {[all | vlan_name <vlan_name> mac_address <macaddr>]} | ports]

説明

IP-MAC-Port バインディングエントリを表示します。3 種類の情報を参照することができます。

- ip_mac - デバイスの物理アドレスおよび IP アドレスを入力することによって Address Binding エントリを参照することができます。
- blocked - VLAN 名とデバイスの物理アドレスを入力することによって、Blocked Address Binding エントリ（VLAN 名と MAC アドレス間のバインディング）を参照することができます。
- ports - デバイスにおける有効なポート数。

パラメータ

パラメータ	説明
all	IP-MAC-Port バインディングとして、すべての IP-MAC-Port バインディングエントリを指定します。Blocked Address Binding エントリとして、ブロックされるすべての VLAN と連結する物理アドレスを指定します。
<ipaddr>	IP-MAC-Port バインディングが行われるデバイスの IP アドレス。
<macaddr>	IP-MAC-Port バインディングが行われるデバイスの MAC アドレス。

制限事項

なし。

使用例

スイッチの IP-MAC-Port バインディングを参照します。

```
DES-3526:admin#show address_binding ip_mac ipaddress 10.1.1.8 mac_address 00-00-00-00-
00-12
Command: show address_binding ip_mac ipaddress 10.1.1.8 mac_address 00-00-00-00-00-12

ACL_mode     : Enabled
Trap/Log     : Disabled
Enabled ports: 1:1-1:2
IP Address MAC Address       Status   Mode Ports
---------- ----------------- -------- ---- --------
10.1.1.8   00-00-00-00-00-12 Active   ARP  1:1-1:12

Total entries :1

DES-3526:admin#
```

delete address_binding

目的

IP-MAC-Port バインディングエントリを削除します。

構文

delete address_binding [ip-mac [ipaddress <ipaddr> mac_address <macaddr> | all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]

説明

IP-MAC-Port バインディングエントリを削除します。2 種類の情報を削除することができます。

- ip_mac - デバイスの物理アドレス、および IP アドレスを入力することによって Address Binding エントリを削除することができます。「all」を指定すると、すべての Address Binding エントリを削除します。
- blocked - VLAN 名とデバイスの物理アドレスを入力することによって、Blocked Address Binding エントリ（VLAN 名と MAC アドレス間のバインディング）を削除することができます。「all」を指定すると、すべての Blocked Address Binding エントリを削除します。

パラメータ

パラメータ	説明
<ipaddr>	IP-MAC-Port バインディングが行われるデバイスの IP アドレス。
<macaddr>	IP-MAC-Port バインディングが行われるデバイスの MAC アドレス。
<vlan_name>	既知の VLAN で特定のデバイスをブロックするために MAC アドレスに割り当てられる VLAN の名前。
all	IP-MAC-Port バインディングとして、すべての IP-MAC-Port バインディングエントリを指定します。Blocked Address Binding エントリとして、ブロックされるすべての VLAN と連結する物理アドレスを指定します。

制限事項

管理者レベルユーザおよびオペレータレベルのみ本コマンドを実行できます。

使用例

スイッチの IP-MAC Binding を削除します。

```
DES-3526:admin#delete address-binding ip-mac ipaddress 10.1.1.1 mac_address 00-00-00-00-
00-06
Command: delete address-binding ip-mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-06

Success.

DES-3526:admin#
```

enable address_binding acl_mode

目的

IP-MAC-Port バインディングエントリの ACL モードを有効にします。

構文

enable address_binding acl_mode

説明

以前の設定を変更せずにスイッチの IP-MAC-Port バインディングの ACL モードを「enable」（有効）にします。有効にすると、スイッチは、「show access_profile」コマンドを使用して参照可能な 2 つの ACL パケットコンテンツマスクエントリを自動的に作成します。この 2 つの ACL エントリは特定の IP-MAC-Port バインディングを作成します。

パラメータ

なし。

制限事項

管理者レベルユーザおよびオペレータレベルのみ本コマンドを実行できます。アクセスプロファイルテーブルが使用可能な 14 エントリ内に 2 つの有効なエントリを持つ場合、このコマンドの有効時に作成された ACL エントリだけが自動的にインストールされます。これらのアクセスプロファイルエントリは、「delete access_profile profile_id」ではなく、「disable address_binding acl_mode」コマンドを使用して削除されます。また、「show config」コマンドでは、IP-MAC ACL モードアクセスプロファイルエントリを作成するコマンドを表示しません。

使用例

IP-MAC Binding ACL モードを有効にします。

```
DES-3526:admin#enable address_binding acl_mode
Command: enable address_binding acl_mode

Success.

DES-3526:admin#
```

disable address_binding acl_mode

目的

IP-MAC-Port バインディングエントリの ACL モードを無効にします。

構文

disable address_binding acl_mode

説明

以前の設定を変更せずにスイッチの IP-MAC-Port バインディングの ACL モードを「disable」（無効）にします。無効にすると、スイッチは、「show access_profile」コマンドを使用して参照可能な 2 つの ACL パケットコンテンツマスクエントリを自動的に削除します。

パラメータ

なし。

制限事項

管理者レベルユーザおよびオペレータレベルのみ本コマンドを実行できます。アクセスプロファイルテーブルが使用可能な 14 エントリ内に 2 つの有効なエントリを持つ場合、このコマンドの有効時に作成された ACL エントリだけが自動的にインストールされます。これらのアクセスプロファイルエントリは、「delete access_profile profile_id」ではなく、「disable address_binding acl_mode」コマンドを使用して削除されます。また、「show config」コマンドでは、IP-MAC ACL モードアクセスプロファイルエントリを作成するコマンドを表示しません。

使用例

IP-MAC Binding ACL モードを無効にします。

```
DES-3526:admin#disable address_binding acl_mode
Command: disable address_binding acl_mode

Success.

DES-3526:admin#
```

enable address_binding trap_log

目的

IP-MAC-Port バインディング機能のトラップログを有効にします。

構文

enable address_binding trap_log

説明

IP-MAC-Port バインディングのトラップログメッセージの送信を「enable」（有効）にします。有効にすると、スイッチはスイッチに設定された IP-MAC-Port バインディングに一致しない ARP パケットを受信した場合に、SNMP エージェントとスイッチログにトラップログメッセージを送信します。

パラメータ

なし。

制限事項

管理者レベルユーザおよびオペレータレベルのみ本コマンドを実行できます。

使用例

スイッチの IP-MAC-Port バインディングトラップログメッセージの送信を有効にします。

```
DES-3526:admin#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DES-3526:admin#
```

disable address_binding trap_log

目的

IP-MAC-Port バインディング機能のトラップログを無効にします。

構文

disable address_binding trap_log

説明

IP-MAC-Port バインディングのトラップログメッセージの送信を「disable」（無効）にします。

パラメータ

なし。

制限事項

管理者レベルユーザおよびオペレータレベルのみ本コマンドを実行できます。

使用例

スイッチの IP-MAC-Port バインディングトラップログメッセージの送信を無効にします。

```
DES-3526:admin#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DES-3526:admin#
```

第 19 章　基本 IP コマンド

コマンドラインインタフェース（CLI）における基本 IP コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config ipif	<ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} bootp | dhcp]
show ipif	<ipif_name 12>

次のセクションで各コマンドについて詳しく説明します。

config ipif

目的

IP インタフェースをスイッチに設定します。

構文

config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp]

説明

IP インタフェースをスイッチに設定します。インタフェースごとに 1 つの IPv4 アドレスを追加することができます。

パラメータ

パラメータ	説明
<ipif_name 12>	12 文字以内の半角英数字の文字列を入力して、スイッチの IP インタフェースを識別します。
ipaddress <network_address>	作成する IP アドレスの IP アドレスとネットマスク。既知のフォーマット（例 :10.1.2.3/255.0.0.0 または CIDR フォーマットにおける 10.1.2.3/8）を使用して IP アドレスとマスク情報を指定します。1 つの IPv4 アドレスのみインタフェースに設定できます。
vlan <vlan_name 32>	上記 IP インタフェースに対応する VLAN 名を入力します。
state [enable | disable]	IP インタフェースを「enable」（有効）または「disable」（無効）にします。
bootp	スイッチのシステム IP インタフェースに IP アドレスを割り当てるために、BOOTP プロトコルを選択します。本方式は IPv4 アドレス専用であり、手動で IPv4 アドレスを設定し、このパラメータを指定すると、設定された IP アドレスはこのプロトコルによって自動的に上書きされます。
dhcp	スイッチのシステム IP インタフェースに IP アドレスを割り当てるために、DHCP プロトコルを選択します。autoconfig 機能を使用している場合、スイッチが自動的に DHCP クライアントとなるため、ipif 設定を変更する必要はありません。本方式は IPv4 アドレス専用であり、手動で IPv4 アドレスを設定し、このパラメータを指定すると、設定された IP アドレスはこのプロトコルによって自動的に上書きされます。

制限事項

管理者レベルまたはオペレータレベルユーザのみ本コマンドを実行できます。

使用例

IPv4 インタフェースシステムを設定します。

```
DES-3526:admin#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DES-3526:admin#
```

show ipif

目的

スイッチの IP インタフェース設定を表示します。

構文

show ipif {<ipif_name 12>}

説明

スイッチの IP インタフェース設定を表示します。

パラメータ

パラメータ	説明
<ipif_name 12>	表示する作成済みの IP インタフェース名

制限事項

なし。

使用例

IP インタフェース設定を表示します。

```
DES-3526:admin#show ipif System
Command: show ipif System

Interface Name              :System
VLAN Name                   :default
Interface Admin State       :Enabled
IPv4 Address                :10.53.13.199/8 (Manual)   Primary

Total Entries :1

DES-3526:admin#
```

第 20 章　IGMP Snooping コマンド

コマンドラインインタフェース（CLI）における IGMP Snooping コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config igmp_snooping	[<vlan_name 32> | all] {host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 0-16711450> | state [enable | disable]}
config igmp_snooping querier	[<vlan_name 32> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable | disable]}
config router_ports	<vlan_name 32> [add | delete] <portlist>
config router_ports forbidden	<vlan_name 32> [add | delete] <portlist>
enable igmp snooping	forward_mcrouter_only
show igmp snooping	vlan <vlan_name 32>
disable igmp snooping	
show igmp snooping group	vlan <vlan_name 32>
show router ports	{vlan <vlan_name 32>} {static | dynamic | forbidden}
show igmp_snooping forwarding	{vlan <vlan_name 32>}
show igmp_snooping group	{vlan <vlan_name 32>}
create igmp_snooping　multicast_vlan	<vlan_name 32><vlanid 2-4094>
config igmp_snooping　multicast_vlan	<vlan_name 32> {member_port <portlist> | source_port <portlist> | state　[enable | disable] | replace_source_ip [ipaddr]}
delete igmp_snooping multicast_vlan	<vlan_name 32>
show igmp_snooping multicast_vlan	{<vlan_name 32>}

次のセクションで各コマンドについて詳しく説明します。

config igmp_snooping

目的

スイッチに IGMP Snooping を設定します。

構文

config igmp_snooping [<vlan_name 32> |all] { host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 0-16711450> | state [enable|disable]}

説明

スイッチに IGMP Snooping を設定します。

パラメータ

パラメータ	説明
vlan <vlan_name 32> | all	IGMP Snooping を設定する VLAN 名。「all」はすべての VLAN を示します。
host_timeout <sec 1-16711450>	スイッチが Host membership report を受信しない場合に、ホストがマルチキャストグループのメンバで居続ける最大時間（秒）。初期値は 260（秒）です。
router_timeout <sec 1-16711450>	スイッチが Host membership report を受信しない場合に、ルータがマルチキャストグループのメンバで居続ける最大時間（秒）。初期値は 260（秒）です。
leave_timer <sec 1-16711450>	leave group メッセージを送信した後に、マルチキャストアドレスが削除されずにデータベースに保持される時間。初期値は 2（秒）です。
state [enable | disable]	指定された VLAN の IGMP Snooping を「enable」（有効）または「disable」（無効）にします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IGMP Snooping を設定します。

```
DES-3526:admin#config igmp_snooping vlan default host_timeout 250 state enable
Command: config igmp_snooping vlan default host_timeout 250 state enable

Success.

DES-3526:admin#
```

config router_ports

目的

ルータポートとしてポートを設定します。

構文

config router_ports <vlan_name 32> [add | delete] <portlist>

説明

マルチキャストが有効なルータに接続するポート範囲を指定します。これは、宛先として本ルータが持つすべてのパケットをプロトコルなどにかかわらず、マルチキャストが有効なルータに到達するように設定します。

パラメータ

パラメータ	説明
<vlan_name 32>	ルータポートが存在する VLAN 名。
add | delete	指定した VLAN にルータポートを追加または削除します。
<portlist>	ルータポートとして設定するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スタティックルータポートを設定します。

```
DES-3526:admin#config router_ports default add 1:1-1:10
Command: config router_ports default add 1:1-1:10

Success.

DES-3526:admin#
```

config router_ports_forbidden

目的

マルチキャスト禁止ルータポートとしてポートを設定します。

構文

config router_ports_forbidden <vlan_name 32> [add | delete] <portlist>

説明

マルチキャストが禁止されるルータのポート範囲を指定します。これは、宛先として本ルータが持つすべてのパケットをプロトコルなどにかかわらず、マルチキャストがルータに到達しないように設定します。

パラメータ

パラメータ	説明
<vlan_name 32>	ルータポートが存在する VLAN 名。
add | delete	指定した VLAN にルータポートを追加または削除します。
<portlist>	ルータポートとして設定するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スタティックルータポートを設定します。

```
DES-3526:admin#config router_ports_forbidden default add 2-10
Command: config router_ports_forbidden default add 2-10

Success.

DES-3526:admin#
```

enable igmp_snooping

目的

スイッチの IGMP Snooping を有効にします。

構文

enable igmp_snooping {forward_mcrouter_only}

説明

スイッチの IGMP Snooping を有効にします。「forward_mcrouter_only」が指定されると、すべてのマルチキャストトラフィックはマルチキャストルータ宛てに送信されます。「forward_mcrouter_only」が指定されないと、マルチキャストトラフィックはすべての IP ルータ宛てに送信されます。

パラメータ

パラメータ	説明
forward_mcrouter_only	スイッチはマルチキャストが有効なルータにのみ、マルチキャストトラフィックを送信します。それ以外の場合、マルチキャストトラフィックはすべての IP ルータ宛てに送信されます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチに IGMP Snooping を有効にします。

```
DES-3526:admin#enable igmp_snooping
Command: enable igmp_snooping

Success.

DES-3526:admin#
```

disable igmp_snooping

目的

スイッチの IGMP Snooping を無効にします。

構文

disable igmp_snooping {forward_mcrouter_only}

説明

スイッチの IGMP Snooping を無効にします。IP マルチキャストルーティングが使用されていない場合にだけ、IGMP Snooping を無効にすることができます。IGMP Snooping を無効にすると、すべての IGMP と IP マルチキャストトラフィックは与えられた IP インタフェースでフラッドします。

パラメータ

パラメータ	説明
forward_mcrouter_only	コマンドに本パラメータを追加すると、マルチキャストが有効なルータへのすべてのマルチキャストトラフィック送信を無効にします。スイッチは、全マルチキャストトラフィックをすべての IP ルータ宛てに送信します。 本コマンドをパラメータなしで入力すると、スイッチの IGMP Snooping を無効にします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチの IGMP Snooping を無効にします。

```
DES-3526:admin#disable igmp_snooping
Command: disable igmp_snooping

Success.

DES-3526:admin#
```

マルチキャストが有効なルータに対するマルチキャストトラフィック送信を無効にします。

```
DES-3526:admin#disable igmp_snooping forward_mcrouter_only
Command: disable igmp_snooping forward_mcrouter_only

Success.

DES-3526:admin#
```

show igmp_snooping

目的

スイッチの現在の IGMP Snooping ステータスを表示します。

構文

show igmp_snooping {vlan <vlan_name 32>}

説明

スイッチの現在の IGMP Snooping ステータスを表示します。

パラメータ

パラメータ	説明
vlan <vlan_name 32>	IGMP Snooping 設定を参照する VLAN 名。

制限事項

なし。

使用例

IGMP Snooping を参照します。

```
DES-3526:admin#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State  :Enabled
Multicast Router Only       :Enabled

 VLAN Name                  :default
 Query Interval             :125
 Max Response Time          :10
 Robustness Value           :2
 Last Member Query Interval :1
 Host Timeout               :250
 Router Timeout             :260
 Leave Timer                :2
 Querier Router Behavior    :Non-Querier
 State                      :Enabled
 Fast Leave                 :Disabled
 Receive Query Count        :0
 Send Query Count           :0

Total Entries:1

DES-3526:admin#
```

show igmp_snooping group

目的

スイッチに設定されている現在の IGMP Snooping 設定を表示します。

構文

show igmp_snooping group {vlan <vlan_name 32>}

説明

スイッチに設定されている現在の IGMP Snooping 設定を表示します。

パラメータ

パラメータ	説明
vlan <vlan_name 32>	IGMP Snooping グループ情報を参照する VLAN 名。

制限事項

なし。

使用例

現在の IGMP Snooping グループを参照します。

```
DES-3526:admin#show igmp_snooping Group
Command: show igmp_snooping Group

VLAN Name        :default
Multicast Group :224.0.0.2
MAC Address      :01-00-5E-00-00-02
Reports          :1
Port Member      :1:2,1:4

VLAN Name        :default
Multicast Group :224.0.0.9
MAC Address      :01-00-5E-00-00-09
Port Member      :1:6, 1:8

Multicast Group :234.5.6.7
MAC Address      :01-00-5E-05-06-07
Reports          :1
Port Member      :1:10, 1:12

Total Entries :3

DES-3526:admin#
```

show router_ports

目的

スイッチに設定されている現在のルータポートを表示します。

構文

show router_ports {vlan <vlan_name 32>}{static|dynamic|forbidden}

説明

スイッチに設定されている現在のルータポートを表示します。

パラメータ

パラメータ	説明
<vlan_name 32>	ルータポートが存在する VLAN 名。
static | dynamic	• static - スタティックに設定されたルータポートを表示します。 • dynamic - ダイナミックに設定されたルータポートを表示します。 • forbidden - 禁止されたルータポートを表示します。

制限事項

なし。

使用例

ルータポートを表示します。

```
DES-3526:admin#show router_ports
Command: show router_ports

 VLAN Name             : default
 Static Router Port    :
 Dynamic Router port   : 3:2

DES-3526:admin#
```

show igmp_snooping forwarding

目的

スイッチ上の現在の IGMP Snooping フォワーディングテーブルのエントリを表示します。

構文

show igmp_snooping forwarding {vlan <vlan_name 32>}

説明

スイッチ上の現在の IGMP Snooping フォワーディングテーブルのエントリを表示します。

パラメータ

パラメータ	説明
<vlan_name 32>	IGMP Snooping フォワーディングテーブル情報を参照する VLAN 名。

制限事項

なし。

使用例

ルータポートを表示します。

```
DES-3526:admin#show igmp_snooping forwarding vlan Marcello
Command: show igmp_snooping forwarding vlan Marcello

 VLAN Name            : Marcello
 Source IP            : 198.19.1.2
 Multicast group      : 239.1.1.1
 Port Member          : 11

Total Entries: 1

DES-3526:admin#
```

create igmp_snooping multicast_vlan

目的

スイッチにマルチキャスト VLAN を作成します。

構文

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>

説明

スイッチにマルチキャスト VLAN を作成します。

パラメータ

パラメータ	説明
<vlan_name 32>	作成するマルチキャスト VLAN 名（半角英数字 32 文字以内）。
<vlanid 2-4094>	作成するマルチキャスト VLAN の VLAN ID。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スタティックルータポートを設定します。

```
DES-3526:admin#create igmp_snooping multicast_vlan accounting 2
Command: create igmp_snooping multicast_vlan accounting 2

Success.

DES-3526:admin#
```

config igmp_snooping multicast_vlan

目的

定義済みのマルチキャスト VLAN を設定します。

構文

config igmp_snooping multicast_vlan <vlan_name 32> {member_port <portlist> | source_port <portlist> | state [enable | disable] {force_agree} | replace_source_ip <ipaddr>}

説明

スイッチの定義済みのマルチキャスト VLAN を設定します。

パラメータ

パラメータ	説明
<vlan_name 32>	IGMP Snooping を設定するマルチキャスト VLAN 名（半角英数字 32 文字以内）。
member_port <portlist>	マルチキャスト VLAN に追加するポートリストを入力します。メンバポートはマルチキャスト VLAN のタグなしメンバになります。
source_port <portlist>	マルチキャスト VLAN に追加するポートリストを入力します。送信元ポートはマルチキャスト VLAN のタグ付きメンバになります。
state [enable | disable] {force_agree}	マルチキャスト VLAN を有効または無効にします。 ・force_agree - 設定を強制します。
replace_source-ip [ipaddr]	変更する IP アドレスを入力します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スタティックルータポートを設定します。

```
DES-3526:admin#config igmp_snooping multicast_vlan accounting member_port 4-5
source_port 6 state enable
Command: config igmp_snooping multicast_vlan accounting member_port 4-5 source_
port 6 state enable

Success.

DES-3526:admin#
```

delete igmp_snooping multicast_vlan

目的

定義済みのマルチキャスト VLAN を削除します。

構文

delete igmp_snooping multicast_vlan <vlan_name 32>

説明

定義済みのマルチキャスト VLAN を削除します。

パラメータ

パラメータ	説明
<vlan_name 32>	削除するマルチキャスト VLAN 名（半角英数字 32 文字以内）。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

マルチキャスト VLAN を削除します。

```
DES-3526:admin#delete igmp_snooping multicast_vlan accounting
Command: delete igmp_snooping multicast_vlan accounting

Success.

DES-3526:admin#
```

show igmp_snooping multicast_vlan

目的

スイッチのマルチキャスト VLAN 設定を表示します。

構文

show igmp_snooping multicast_vlan {<vlan_name 32>}

説明

スイッチのマルチキャスト VLAN 設定を表示します。

パラメータ

パラメータ	説明
<vlan_name 32>	表示するマルチキャスト VLAN 名（半角英数字 32 文字以内）。

制限事項

なし。

使用例

マルチキャスト VLAN を参照します。

```
DES-3526:admin#show igmp_snooping multicast_vlan accounting
Command: snow igmp_snooping multicast_vlan accounting

VID               : 2          VLAN Name     : accounting
Member Ports      : 4-5
Source Ports      : 6
Status            : Enabled
Replace Source IP : 0.0.0.0

DES-3526:admin#
```

第 21 章　DHCP リレーコマンド

コマンドラインインタフェース（CLI）における DHCP リレーコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config dhcp_relay	{hops <value 1-16> | time <sec 0-65535>}
config dhcp_relay add ipif	<ipif_name 12> <ipaddr>
config dhcp_relay delete ipif	<ipif_name 12> <ipaddr>
config dhcp_relay option_82 state	[enable | disable]
config dhcp_relay option_82 check	[enable | disable]
config dhcp_relay option_82 policy	[replace | drop | keep]
show dhcp_relay	{ipif <ipif_name 12>}
enable dhcp_relay	
disable dhcp_relay	

以下のセクションで各コマンドについて詳しく説明します。

config dhcp_relay

目的

スイッチの DHCP/BOOTP リレー機能を設定します。

構文

config dhcp_relay [hops <value 1-16> | time <sec 0-65535>]

説明

DHCP/BOOTP リレー機能を設定します。

パラメータ

パラメータ	説明
hops <value 1-16>	DHCP パケットが越えることができるリレーエージェントの最大ホップ数を指定します。
time <sec 0-65535>	この時間を経過すると、スイッチは DHCP パケットをリレーします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

DHCP リレーを設定します。

```
DES-3526:admin#config dhcp_relay hops 2 time 23
Command: config dhcp_relay hops 2 time 23

Success.

DES-3526:admin#
```

config dhcp_relay add ipif

目的

スイッチの DHCP/BOOTP リレーテーブルに送信先 IP アドレスを追加します。

構文

config dhcp_relay add ipif <ipif_name 12> <ipaddr>

説明

DHCP/BOOTP リレーパケットを転送（リレー）する送信先として IP アドレスを追加します。

パラメータ

パラメータ	説明
<ipif_name 12>	DHCP リレーを有効にする IP インタフェース名。
<ipaddr>	DHCP サーバの IP アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

```
DES-3526:admin#config dhcp_relay add ipif System 10.58.44.6
Command: config dhcp_relay add ipif System 10.58.44.6

Success.

DES-3526:admin#
```

config dhcp_relay delete ipif

目的

スイッチの DHCP/BOOTP リレーテーブルから送信先 IP アドレスを 1 個またはすべて削除します。

構文

config dhcp_relay delete ipif <ipif_name 12> <ipaddr>

説明

スイッチの DHCP/BOOTP リレーテーブルから送信先 IP アドレスを削除します。

パラメータ

パラメータ	説明
<ipif_name 12>	以下の IP アドレスを含む IP インタフェース名。
<ipaddr>	DHCP サーバの IP アドレス。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

DHCP/BOOTP リレーテーブルから送信先 IP アドレスを削除します。

```
DES-3526:admin#config dhcp_relay delete ipif System 10.58.44.6
Command: config dhcp_relay delete ipif System 10.58.44.6

Success.

DES-3526:admin#
```

config dhcp_relay option_82 state

目的

スイッチの DHCP リレーエージェント Information Option 82 の状態を設定します。

構文

config dhcp_relay option_82 state [enable | disable]

説明

スイッチの DHCP リレーエージェント Information Option 82 の状態を設定します。リレーエージェントは DHCP サーバとクライアント間で交わすメッセージに DHCP Relay Information（Option 82 フィールド）を挿入 / 削除します。リレーエージェントが DHCP リクエストを受信すると、Option 82 情報と（設定があれば）リレーエージェントの IP アドレスをパケットに付加します。Option 82 情報が付加されたパケットは DHCP サーバに送信されます。パケットを受信し、サーバが Option-82 をサポートしている場合、サーバは remote ID または circuit ID に割り当て可能な IP アドレス数の制限などのポリシーを適用します。DHCP サーバは、DHCP リプライ内の Option-82 フィールドをエコーバックします。DHCP サーバは、スイッチが DHCP リクエストを中継していた場合はユニキャストで応答します。スイッチは Option-82 情報が挿入されていたことを確認します。最後にリレーエージェントは、Option-82 フィールドを削除し、DHCP リクエストを送信した DHCP クライアントに接続しているスイッチポートにそのパケットを転送します。

パラメータ

パラメータ	説明
enable	パケットへの Option-82 情報の付加を有効にします。
disable	リレーエージェントは DHCP サーバとクライアント間で交換するメッセージに DHCP Relay Information（Option 82 フィールド）の挿入 / 削除を行いません。また、Option 82 の Check と Policy のフィールドは無効になります。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

DHCP Relay Agent Information Option 82 State を設定します。

```
DES-3526:admin#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DES-3526:admin#
```

config dhcp_relay option_82 check

説明

スイッチの DHCP リレーエージェント Information Option 82 のチェックメカニズムを設定します。

構文

config dhcp_relay option_82 check [enable | disable]

説明

スイッチの DHCP リレーエージェント Information Option 82 のチェックメカニズムを設定します。リレーエージェントはパケットの Option 82 フィールドの妥当性のチェックを行います。スイッチが DHCP クライアントから Option 82 フィールドを含むパケットを受信すると、スイッチはこれらのパケットは不正だとしてパケットを廃棄します。リレーエージェントは DHCP サーバから受信したパケットから不正なメッセージを削除します。

パラメータ

パラメータ	説明
enable	パケット内の Option-82 情報の妥当性チェックを有効にします。
disable	リレーエージェントはパケットの Option 82 フィールドの妥当性のチェックを行いません。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

DHCP Relay Agent Information Option 82 Check を設定します。

```
DES-3526:admin#config dhcp_relay option_82 check enable
Command: config dhcp_relay option_82 check enable

Success.

DES-3526:admin#
```

config dhcp_relay option_82 policy

目的

スイッチの DHCP リレーエージェント Information Option 82 のフォワーディングポリシーを設定します。

構文

config dhcp_relay option_82 policy [replace | drop | keep]

説明

スイッチの DHCP リレーエージェント Information Option 82 のフォワーディングポリシーを設定します。

パラメータ

パラメータ	説明
replace	DHCP クライアントから受信したパケットの既存のリレー情報をスイッチの DHCP リレー情報に置き換えます。
drop	DHCP クライアントから受信したパケットに既にリレー情報があった場合はそのパケットを削除します。
keep	DHCP クライアントから受信したパケットの既存のリレー情報を保持します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

DHCP Relay Agent Information Option 82 Policy を設定します。

```
DES-3526:admin#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DES-3526:admin#
```

show dhcp_relay

目的

現在の DHCP/BOOTP リレー設定を表示します。

構文

show dhcp_relay {ipif <ipif_name 12>}

説明

現在の DHCP リレー設定を表示するか、または IP インタフェース名が指定されると、その IP インタフェースの DHCP リレー設定を表示します。

パラメータ

パラメータ	説明
ipif <ipif_name 12>	現在の DHCP リレー設定を表示する IP インタフェース名。

制限事項

なし。

使用例

DHCP リレー設定を表示します。

```
DES-3526:admin#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status                       :Enabled
DHCP/BOOTP Hops Count Limit                   :2
DHCP/BOOTP Relay Time Threshold               :23
DHCP Relay Agent Information Option 82 State  :Enabled
DHCP Relay Agent Information Option 82 Check  :Enabled
DHCP Relay Agent Information Option 82 Policy :Replace

Interface Server 1   Server 2   Server 3   Server 4
--------- ---------- ---------- ---------- ----------
System    10.58.44.6

DES-3526:admin#
```

使用例

DHCP リレー設定の 1 つの送信先アドレスについて表示します。

```
DES-3526:admin#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/BOOTP Relay Status                       :Enabled
DHCP/BOOTP Relay Time Threshold               :23
DHCP Relay Agent Information Option 82 Check :Enabled
Interface Server 1   Server 2   Server 3   Server 4
--------- ---------- ---------- ---------- ----------

DES-3526:admin#
```

enable dhcp_relay

目的

スイッチの DHCP/BOOTP リレーを有効にします。

構文

enable dhcp_relay

説明

スイッチの DHCP/BOOTP リレーを有効にします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

DHCP リレーを有効にします。

```
DES-3526:admin#enable dhcp_relay
Command:enable dhcp_relay

Success.

DES-3526:admin#
```

disable dhcp_relay

目的

スイッチの DHCP/BOOTP リレー機能を無効にします。

構文

disable dhcp_relay

説明

スイッチの DHCP/BOOTP リレー機能を無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

DHCP リレーを無効にします。

```
DES-3526:admin#disable dhcp_relay
Command: disable dhcp_relay

Success.

DES-3526:admin#
```

第 22 章　IP マルチキャスト範囲の限定コマンド

IP マルチキャスト範囲の限定コマンドでは、マルチキャストアドレス範囲を指定することで、ポートまたはポート範囲へのアクセスを許可（Permit）または拒否（Deny）することが可能です。

コマンドラインインタフェース（CLI）における IP マルチキャスト範囲の限定コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create multicast_range	create multicast_range<range_name> {from <multicast_ipaddr> to <multicast_ipaddr>
delete multicast_range	delete multicast_range<range_name>
show multicast_range	<range_name>
config limited multicast address	<portlist> {add [multicast_range] | delete [multicast_range] | access [permit | deny] | state [enable | disable]}
show limited multicast address	{<portlist>}

次のセクションで各コマンドについて詳しく説明します。

create multicast_range

目的

識別名を持つマルチキャスト IP アドレスの範囲を作成します。

構文

create multicast_range<range_name> {from <multicast_ipaddr> to <multicast_ipaddr>

説明

識別名を持つマルチキャスト IP アドレスの範囲を作成します。作成すると、この範囲名をスイッチが許可または拒否するマルチキャストアドレスの一覧を作成する「config limited_multicast_addr」コマンドに追加できます。

パラメータ

パラメータ	説明
<range_name>]	マルチキャスト範囲を識別するために使用する名前を入力します。
from <multicast_ipaddr>	マルチキャスト範囲の開始 IP アドレスを入力します。
to <multicast_ipaddr>	マルチキャスト範囲の終了 IP アドレスを入力します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

ポート 1-3 に IP マルチキャストの限定機能を設定します。

```
DES-3526:admin#create multicast_range M-Range-2 from 224.1.1.1 to 230.1.1.1
Command: create multicast_range M-Range-2 from 224.1.1.1 to 230.1.1.1
Success.
DES-3526:admin#
```

delete multicast_range

目的

識別名を持つマルチキャスト IP アドレスの範囲を削除します。

構文

delete multicast_range [<range_name> | all]

説明

「create multicast_range」コマンドで作成したマルチキャスト範囲を削除します。

パラメータ

パラメータ	説明
[<range_name> | all]	<range_name> - 削除するマルチキャスト範囲を入力します。 all - 全てのマルチキャストを削除します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

M-Range-2 の IP マルチキャストを削除します。

```
DES-3526:admin#delete multicast_range M-Range-2
Command: delete multicast_range M-Range-2
Success.
DES-3526:admin#
```

show multicast_range

目的

識別名を持つマルチキャスト IP アドレスの範囲を表示します。

構文

show multicast_range <range_name>

説明

「create multicast_range」コマンドで作成したマルチキャスト範囲を表示します。

パラメータ

パラメータ	説明
<range_name>]	表示するマルチキャスト範囲を入力します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

IP マルチキャストの範囲を表示します。

```
DES-3526:admin#show multicast_range
Command: show multicast_range
No. Name From To
---- ---------------- ---------------- ----------------
1 M-Range-1 224.0.0.0 239.0.0.0
2 M-Range-2 224.1.1.1 230.1.1.1
Total Entries : 2
DES-3526:admin#
```

config limited multicast address

目的

定義済みのマルチキャストアドレス範囲に（から）ポートを追加または削除します。また、スイッチからのその範囲へのアクセスを許可または拒否します。

構文

config limited multicast address <portlist> [add multicast_range <range_name> | delete multicast_range [<range_name>|all] | {access [permit | deny] | state [enable | disable]}]

説明

マルチキャスト範囲に次のタスクを実行します。スイッチポートをマルチキャスト範囲に（から）追加または削除し、さらにスイッチへのアクセスをこれらのマルチキャストアドレスに許可または制限します。

パラメータ

パラメータ	説明
<portlist>	マルチキャスト範囲にポートリストを追加します。ポートの範囲は、「-」(ダッシュ) を使用して指定します。続き番号ではないポートリストエントリは「、」(カンマ) で分けます。(例 :1:1-1:3,1:7-1:9)
[add multicast_range <range_name> | delete multicast_range <range_name> | all]	add - 続くパラメータに従って、指定のマルチキャスト範囲にポートを追加します。 delete - 続くパラメータに従って、指定のマルチキャスト範囲からポートを削除します。 - <range_ name> - マルチキャスト範囲名を入力します。 - all - 全てにマルチキャストに指定します。
access [permit | deny]	続くパラメータに基づき、ポートのマルチキャストアドレスへのアクセスを許可または拒否します。 • permit - このマルチキャスト範囲に対して、スイッチへのアクセスを許可します。 • deny - このマルチキャスト範囲に対して、スイッチからのアクセスを拒否します。
state [enable | disable]	マルチキャスト設定を有効または無効にします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

マルチキャスト範囲ポート 1-3 の設定を変更します。

```
DES-3526:admin#config limited_multicast_addr ports 1 accesspermit state enable
Command: config limited_multicast_addr ports 1 access permit state enable
Success.
DES-3526:admin#
```

show limited_multicast_addr

目的

ポートごとにマルチキャストアドレス範囲を表示します。

構文

show limited_multicast_addr {ports <portlist>}

説明

ポートごとにマルチキャストアドレス範囲を表示します。

パラメータ

パラメータ	説明
{ports <portlist>}	IP マルチキャスト範囲の限定機能を表示するポートまたはポート範囲。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。例えば、1:3-2:4 は、スイッチ 1 のポート 3 とスイッチ 2 のポート 4 間にあるすべてのポートを表しています。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

なし。

使用例

ポート 1-3 のマルチキャスト範囲を表示します。

```
DES-3526:admin#show limited multicast_addr ports 1-3
Command: show limited multicast_addr ports 1-3
Port From To Access Status
---- -------------- --------------- -------- -------
1 224.1.1.1 224.1.1.2 permit enable
2 224.1.1.1 224.1.1.2 permit enable
3 224.1.1.1 224.1.1.2 permit enable
DES-3526:admin#
```

第 23 章　802.1X コマンド

本スイッチは、IEEE 802.1X ポートベースおよびMACベースのネットワークアクセスコントロールのサーバ機能を実装しています。このメカニズムは、ポートがフレームの送受信の前に一致する必要のあるスイッチの各ポートの基準を設定することで、認証ユーザまたは他のネットワークデバイスにネットワークリソースへのアクセスを許可するものです。

コマンドラインインタフェース（CLI）における 802.1X コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable 802.1x	
disable 802.1x	
show 802.1x auth_state	{ports <portlist>}
show 802.1x auth_configuration	{ports <portlist>}
config 802.1x capability ports	[<portlist> | all] [authenticator | none]
config 802.1x auth_parameter ports	[<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1- 65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | enable_reauth [enable | disable]}]
config 802.1x auth_protocol	[radius eap | radius pap]
config 802.1x init	{port_based ports [<portlist> | all] | mac_based [ports] [<portlist> |all] {mac_address <macaddr>}]
config 802.1x auth_mode	[port_based | mac_based]
config 802.1x reauth	{port_based ports [<portlist> | all] | mac_based [ports] [<portlist> | all] {mac_address <macaddr>}]
config radius add	<server_index 1-3> <server_ip> key <passwd 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}]
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> {ipaddress <server_ip> | key <passwd 32> [auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>]}
show radius	
create 802.1x guest_vlan	<vlan_name 32>
config 802.1x guest_vlan ports	[<portlist> | all] state [enable | disable]
delete 802.1x guest_vlan	{<vlan_name 32>}
show 802.1x guest_vlan	

次のセクションで各コマンドについて詳しく説明します。

enable 802.1x

目的

スイッチの 802.1X ネットワークアクセスコントロールのサーバアプリケーションを有効にします。

構文

enable 802.1x

説明

スイッチの 802.1X ネットワークアクセスコントロールのサーバアプリケーションを有効にします。「config 802.1x auth_mode」コマンドを使用して、ポートベースまたは MAC ベースを選択します。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチの 802.1X 機能を有効にします。

```
DES-3526:admin#enable 802.1x
Command: enable 802.1x

Success.

DES-3526:admin#
```

disable 802.1x

目的

スイッチの 802.1X サーバを無効にします。

構文

disable 802.1x

説明

スイッチの 802.1X ネットワークアクセスコントロールのサーバアプリケーションを無効にします。「config 802.1x auth_mode」コマンドを使用して、ポートベースまたは MAC ベースを選択します。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチの 802.1X を無効にします。

```
DES-3526:admin#disable 802.1x
Command: disable 802.1x

Success.

DES-3526:admin#
```

show 802.1x auth_configuration

目的

スイッチにおける 802.1X サーバの現在の設定を表示します。

構文

show 802.1x auth_configuration {ports <portlist>}

説明

スイッチに現在設定されている 802.1X ポートベースまたは MAC ベースのネットワークアクセスコントロールローカルユーザを表示します。

パラメータ

パラメータ	説明
ports <portlist>	• <portlist> - 表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

以下のパラメータが表示されます。

パラメータ	説明
802.1x : Enabled / Disabled	スイッチの 802.1X 機能の現在のステータスを表示します。
Authentication Mode	MAC アドレスまたはポートごとに認証モードを表示します。
Authentication Protocol : Radius_EAP	スイッチと RADIUS サーバ間で使用している認証プロトコルを表示します。Radius_EAP または Radius_PAP をと表示される可能性があります。
Port number	スイッチの物理ポート番号を表示します。
Capability : Authenticator/None	上で表示されたポート番号の 802.1X 機能について表示します。スイッチに設定できる 802.1X 機能には、Authenticator と None の 2 つのタイプがあります。
AdminCtlDir : Both / In	未認証の制御ポートが送受両方向または受信方向だけで通信に制御を行うかどうかを表示します。
OpenCtlDir : Both / In	未認証の制御ポートが送受両方向または受信方向だけで通信に制御を行うかどうかを表示します。
Port Control	ポートの認証ステータスに対する管理用の制御を表示します。 • ForceAuth - ポートのオーセンティケータを Authorized 状態にします。 • ForceUnauth - ポートを Unauthorized 状態にします。
QuietPeriod	認証に失敗した後、新しく認証を開始するまでの間隔を表示します。
TxPeriod	EAP Request/Identity パケットを送信するためにサプリカント（ユーザ）からの応答を待つ時間を表示します。
SuppTimeout	Request / Identity パケットを除くすべての EAP パケットに対するサプリカント（ユーザ）からの応答を待つ時間を表示します。
ServerTimeout	RADIUS サーバからの応答を待つ時間を表示します。
MaxReq	サプリカントへのパケットの再送信回数を表示します。
ReAuthPeriod	連続する再認証の間隔を表示します。
ReAuthenticate : Enabled / Disabled	再認証を行うかどうかを表示します。

制限事項

なし。

使用例

802.1X 認証状態を表示します。

```
DES-3526:admin#show 802.1x auth_configuration ports 1:1
Command: show 802.1x auth_configuration ports 1:1

802.1X                  :Enabled
Authentication Mode     :Port_based
Authentication Protocol :RADIUS_EAP

Port number    :1:1
Capability     :None
AdminCrlDir    :Both
OpenCrlDir     :Both
Port Control   :Auto
QuietPeriod    :60 sec
TxPeriod       :30 sec
SuppTimeout    :30 sec
ServerTimeout  :30 sec
MaxReq         :2 times
ReAuthPeriod   :3600 sec
ReAuthenticate :Disabled

CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

show 802.1x auth_state

目的

スイッチにおける 802.1X サーバの現在の認証状態を表示します。

構文

show 802.1x auth_state {ports <portlist> }

説明

スイッチにおける 802.1X ポートベースまたは MAC ベースネットワークアクセスサーバアプリケーションの現在の認証状態を表示します。

パラメータ

パラメータ	説明
ports <portlist>	• <portlist> - 表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

以下のパラメータが表示されます。

パラメータ	説明
Auth PAE State	Authenticator PAE の状態を表示します。（Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth）
Backend State	Backend Authenticator の現在の状態を表示します。（Request / Response / Fail / Idle / Initialize / Success / Timeout）
Port Status	認証処理の結果を表示します。 • Authorized - ユーザが認証され、ネットワークにアクセスできます。 • Unauthorized - ユーザが認証されず、ネットワークにアクセスできません。

制限事項

なし。

使用例

ポートベースの 802.1X の 802.1X auth 状態を表示します。

```
DES-3526:admin#show 802.1x auth_state
Command: show 802.1x auth_state

Port Auth PAE State Backend State Port Status
---- -------------- ------------- -----------
1:1  ForceAuth      Success       Authorized
1:2  ForceAuth      Success       Authorized
1:3  ForceAuth      Success       Authorized
1:4  ForceAuth      Success       Authorized
1:5  ForceAuth      Success       Authorized
1:6  ForceAuth      Success       Authorized
1:7  ForceAuth      Success       Authorized
1:8  ForceAuth      Success       Authorized
1:9  ForceAuth      Success       Authorized
1:11 ForceAuth      Success       Authorized
1:12 ForceAuth      Success       Authorized
1:13 ForceAuth      Success       Authorized
1:14 ForceAuth      Success       Authorized
```

MAC ベースの 802.1X の 802.1X auth 状態を表示します。

```
DES-3526:admin#show 802.1x auth_state
Command: show 802.1x auth_state

Port number :1:1
 Index MAC Address       Auth PAE State Backend State Port Status
 ----- ----------------- -------------- ------------- -----------
 1     00-08-02-4E-DA-FA Authenticated  Idle          Authorized
 2
 3
 4
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
 16
```

config 802.1x auth_mode

目的

スイッチの 802.1X 認証モードを設定します。

構文

config 802.1x auth_mode [port_based | mac_based]

説明

スイッチにポートベースまたは MAC ベースの 802.1X 認証機能を有効にします。

パラメータ

パラメータ	説明
[port_based | mac_based]	ポートか MAC アドレスによる 802.1X 認証をします。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

MAC アドレスによる 802.1X 認証を設定します。

```
DES-3526:admin#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

DES-3526:admin#
```

config 802.1x capability ports

目的

ポート範囲による 802.1X 認証を設定します。

構文

config 802.1x capability ports [<portlist> | all] [authenticator | none]

説明

各ポートに設定可能な 4 つのパラメータがあります。Authenticator、Supplicant、Authenticator および Supplicant、None です。

パラメータ

パラメータ	説明
<portlist> l all	• <portlist> - 表示するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - スイッチのすべてのポートを指定します。
authenticator | none	• authenticator - ネットワークのアクセス権を取得するために認証プロセスを通過する必要があります。 • none - ポートは 802.1X 機能によって制御されません。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

モジュール 1 のポート 1-10 に 802.1X 機能を設定します。

```
DES-3526:admin#config 802.1x capability ports 1:1-1:10 authenticator
Command: config 802.1x capability ports 1:1-1:10 authenticator

Success.

DES-3526:admin#
```

config 802.1x auth_parameter ports

目的

ポート範囲に 802.1X 認証パラメータを設定します。デフォルトパラメータは、指定した範囲内のすべてのポートをデフォルト 802.1X 設定に戻します。

構文

config 802.1x auth_parameter ports [<portlist>|all] [default|{direction [both|in]|port_control [force_unauth|auto|force_auth]|quiet_period <sec 0-65535>|tx_period <sec 1-65535>|supp_timeout <sec 1-65535>|server_timeout <sec 1-65535>|max_req <value 1-10>|reauth_period <sec 1-65535>|enable_reauth [enable|disable]}]

説明

ポート範囲に 802.1X 認証パラメータを設定します。

パラメータ

パラメータ	説明
<portlist>	表示するポートまたは範囲を指定します。ポートは 802.1X 機能によって制御されません。
all	スイッチのすべてのポートを指定します。
default	指定範囲内のすべてのポートを 802.1X 設定に戻します。
direction [both | in]	制御ポートが送受信両方または受信方向だけの通信をブロックするかどうかを決定します。
port_control	ポート範囲の認証処理における管理用の制御を設定します。以下の認証オプションがあります。 • force_auth - ポートのオーセンティケータを Authorized 状態にします。ネットワークアクセスは許可されます。 • auto - ポートステータスに認証プロセスの結果を反映します。 • force_unauth - ポートを Unauthorized 状態にします。ネットワークアクセスはブロックされます。
quiet_period <sec 0-65535>	認証に失敗した後、新しく認証を開始するまでの間隔を設定します。
tx_period <sec 1-65535>	EAP Request/Identity パケットを送信するためにサプリカント（ユーザ）からの応答を待つ時間を設定します。
supp_timeout <sec 1-65535>	Request/Identity パケットを除くすべての EAP パケットに対するサプリカント（ユーザ）からの応答を待つ時間を設定します。
server_timeout <sec 1-65535>	RADIUS サーバからの応答を待つ時間を設定します。
max_req <value 1-10>	サプリカントへのパケットの再送信回数を設定します。
reauth_period <sec 1-65535>	連続する再認証の間隔を設定します。
enable_reauth [enable | disable]	スイッチが再認証するかどうかを決定します。有効にすると、上記「reauth_period」フィールドで指定した間隔でユーザを再認証します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

モジュール 1 のポート 1-20 に 802.1X 認証パラメータを設定します。

```
DES-3526:admin#config 802.1x auth_parameter ports 1:1-1:20 direction both
Command: config 802.1x auth_parameter ports 1:1-1:20 direction both

Success.

DES-3526:admin#
```

config 802.1x auth_protocol

目的

スイッチの 802.1X 認証プロトコルを設定します。

構文

config 802.1x auth_protocol [radius_eap | radius_pap]

説明

スイッチの 802.1X 認証プロトコルを設定します。

パラメータ

パラメータ	説明
[radius_eap | radius_pap]	認証プロトコルを指定します。

制限事項

管理者レベルのユーザのみ本コマンドを実行できます。

使用例

802.1X 認証プロトコルを設定します。

```
DES-3526:admin# config 802.1x auth_protocol radius_pap
Command: config 802.1x auth_protocol radius_pap
Success.
DES-3526:admin#
```

config 802.1x init

目的

ポート範囲の 802.1X 認証を初期化します。

構文

config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

説明

指定された範囲のポートから操作される指定ポートまたは MAC アドレス範囲の 802.1X 機能をただちに初期化します。

パラメータ

パラメータ	説明
port_based	ポート番号だけに基づいた 802.1X 機能を初期化します。初期化を承認されるポートを指定することができます。
mac_based	MAC アドレスだけに基づいた 802.1X 機能を初期化します。初期化を承認される MAC アドレスを指定することができます。
<portlist> | all	• <portlist> - 設定するポートまたは範囲を指定します。ポートは 802.1X 機能によって制御されません。 • all - スイッチのすべてのポートを指定します。
mac_address <macaddr>	初期化する MAC アドレスを入力します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

すべてのポートの認証状態を初期化します。

```
DES-3526:admin#config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DES-3526:admin#
```

config 802.1x reauth

目的

スイッチの 802.1X 再認証機能を設定します。

構文

config 802.1x reauth [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

説明

スイッチの 802.1X 再認証機能を設定します。

パラメータ

パラメータ	説明
port_based	ポートだけに基づいた 802.1X 再認証機能を設定します。再認証されるポートを指定することができます。
mac_based	MAC アドレスだけに基づいた 802.1X 再認証機能を設定します。再認証される MAC アドレスを指定することができます。
ports <portlist> | all	• <portlist> - 再認証するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - スイッチのすべてのポートを指定します。
mac_address <macaddr>	再認証する MAC アドレスを入力します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

モジュール 1 のポート 1-11 に 802.1X 再認証を設定します。

```
DES-3526:admin#config 802.1x reauth port_based ports 1:1-1:11
Command: config 802.1x reauth port_based ports 1:1-1:11

Success.

DES-3526:admin#
```

config radius add

目的

スイッチが RADIUS サーバと通信するために使用するパラメータを設定します。

構文

config radius add <server_index 1-3> <server_ip> key <passwd 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}]

説明

スイッチが RADIUS サーバと通信するために使用するパラメータを設定します。

パラメータ

パラメータ	説明
<server_index 1-3>	RADIUS サーバの現在の設定に番号を割り当てます。3 つまでの RADIUS サーバ設定のグループをスイッチに入力できます。
<server_ip>	RADIUS サーバの IP アドレス。
key	スイッチと RADIUS サーバ間で使用されるパスワードと暗号キーを指定します。
<passwd 32>	RADIUS サーバとスイッチが使用する共有秘密鍵。32 文字以内で指定します。
default	「auth_port」と「acct_port」設定の両方にデフォルト UDP ポート番号を使用します。
auth_port<udp_port_number 1-65535>	認証リクエストに対する UDP ポート番号。初期値は 1812 です。
acct_port<udp_port_number 1-65535>	アカウンティングリクエストに対する UDP ポート番号。初期値は 1813 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

```
DES-3526:admin#config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

Success.

DES-3526:admin#
```

config radius delete

目的

登録済みの RADIUS サーバ設定を削除します。

構文

config radius delete <server_index 1-3>

説明

登録済みの RADIUS サーバ設定を削除します。

パラメータ

パラメータ	説明
<server_index 1-3>	RADIUS サーバの現在の設定に番号を割り当てます。3 つまでの RADIUS サーバ設定のグループをスイッチに入力できます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

設定済みの RADIUS サーバ通信設定を削除します。

```
DES-3526:admin#config radius delete 1
Command: config radius delete 1

Success.

DES-3526:admin#
```

config radius

目的

スイッチの RADIUS パラメータの設定を行います。

構文

config radius <server_index 1-3> {ipaddress <server_ip> | key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}

説明

スイッチの RADIUS パラメータの設定を行います。

パラメータ

パラメータ	説明
<server_index 1-3>	RADIUS サーバの現在の設定に番号を割り当てます。3 つまでの RADIUS サーバ設定のグループをスイッチに入力できます。
ipaddress <server_ip>	RADIUS サーバの IP アドレス。
key <passwd 32>	スイッチと RADIUS サーバ間で使用されるパスワードと暗号キーを指定します。 RADIUS サーバとスイッチが使用する共有秘密鍵。32 文字以内で指定します。
auth_port <udp_port_number 1-65535>	認証リクエストに対する UDP ポート番号。初期値は 1812 です。
acct_port <udp_port_number 1-65535>	アカウンティングリクエストに対する UDP ポート番号。初期値は 1813 です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

RADIUS パラメータを設定します。

```
DES-3526:admin#config radius 1 10.48.74.121 key dlink
Command: config radius 1 10.48.74.121 key dlink

Success.

DES-3526:admin#
```

show radius

目的

スイッチの現在の RADIUS 設定を表示します。

構文

show radius

説明

スイッチの現在の RADIUS 設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチの現在の RADIUS 設定を表示します。

```
DES-3526:admin#show radius
Command: show radius

Idx IP Address  Auth     Acct      Status Key
               -Port    -Port
               No.       No.
--- ---------- --------- --------- ------ -----
1   10.1.1.1   1812      1813      Active switch
2   20.1.1.1   1800      1813      Active des3500
3   30.1.1.1   1812      1813      Active dlink

Total Entries :3

DES-3526:admin#
```

create 802.1x guest_vlan

目的

設定済みの VLAN を 802.1X ゲスト VLAN として設定します。

構文

create 802.1x guest_vlan <vlan_name 32>

説明

設定済みの VLAN を 802.1X ゲスト VLAN として設定します。ゲスト 802.1X VLAN クライアントは、802.1X に認証されておらず、まだ必要な 802.1X ソフトウェアをインストールしていないが、スイッチに限定的なアクセス権を希望するユーザです。

パラメータ

パラメータ	説明
<vlan_name 32>	802.1X ゲスト VLAN として登録済みの VLAN 名を入力します（半角英数字 32 文字以内）。VLAN は前述の「create vlan」コマンドを使用して作成します。

制限事項

「create vlan」コマンドを使用して作成した VLAN が必要です。1 つの VLAN だけが 802.1X ゲスト VLAN として設定されます。

使用例

設定済みの VLAN を 802.1X ゲスト VLAN として設定します。

```
DES-3526:admin#create 802.1x guest_vlan Trinity
Command: create 802.1x guest_vlan Trinity

Success.

DES-3526:admin#
```

config 802.1x guest_vlan ports

目的

設定済みの 802.1X ゲスト VLAN にポートを設定します。

構文

config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]

説明

802.1 ゲスト VLAN を有効または無効にするために、ポートを設定します。

パラメータ

パラメータ	説明
<portlist> | all	• <portlist> - 設定するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - 802.1X ゲスト VLAN にすべてのポートを設定します。
state [enable | disable]	802.1X ゲスト VLAN が有効または無効になった場合に、ここで指定したポートを有効または無効にします。

制限事項

「create vlan」コマンドを使用して作成した VLAN が必要です。本 VLAN は、ポートベースの 802.1x だけにサポートされています。指定ポートの状態を有効から無効に変更した場合、ポートはデフォルト VLAN に戻ります。

使用例

設定済みの 802.1X ゲスト VLAN ポートを有効に設定します。

```
DES-3526:admin#config 802.1x guest_vlan ports 1:1-1:5 state enable
Command: config 802.1x guest_vlan ports 1:1-1:5 state enable

Success.

DES-3526:admin#
```

show 802.1x guest_vlan

目的

802.1x ゲスト VLAN の設定を参照します。

構文

show 802.1x guest_vlan

説明

802.1X ゲスト VLAN が有効である VLAN の設定を表示します。ゲスト 802.1X VLAN クライアントは、802.1X に認証されておらず、まだ必要な 802.1X ソフトウェアをインストールしていないが、スイッチに限定的なアクセス権を希望するユーザです。

パラメータ

なし。

制限事項

なし。

使用例

設定済みの 802.1X ゲスト VLAN に設定を表示します。

```
DES-3526:admin#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
------------------------------
Guest VLAN              :Trinity
Enable Guest VLAN Ports:1:5-1:8.

DES-3526:admin#
```

delete 802.1x guest_vlan

目的

802.1X ゲスト VLAN を削除します。

構文

delete 802.1x guest_vlan {<vlan_name 32>}

説明

802.1X ゲスト VLAN が有効である VLAN を削除します。ゲスト 802.1X VLAN クライアントは、802.1X に認証されておらず、まだ必要な 802.1X ソフトウェアをインストールしていないが、スイッチに限定的なアクセス権を希望するユーザです。

パラメータ

パラメータ	説明
<vlan_name 32>	削除する 802.1X ゲスト VLAN 名を入力します。(半角英数字 32 文字以内)。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

「create vlan」コマンドを使用して作成した VLAN が必要です。1 つの VLAN だけが 802.1X ゲスト VLAN として設定されます。

使用例

802.1X ゲスト VLAN を削除します。

```
DES-3526:admin#delete 802.1x guest_vlan Trinity
Command: delete 802.1x guest_vlan Trinity

Success.

DES-3526:admin#
```

第 24 章　アクセスコントロールリスト（ACL）コマンド

アクセスプロファイルを作成すると、各パケットヘッダの中の情報に従い、スイッチがパケット送信を決定するための基準を設定できるようになります。VLAN ごとにこれらの基準を指定できます。

アクセスプロファイルの作成は 2 段階に分かれます。最初に「create access_profile」コマンドを使用してアクセスプロファイルを作成します。例えば、サブネット 10.42.73.0 ～ 10.42.73.255 に対して全トラフィックを制限したい場合、はじめにスイッチに対して各フレームの関連フィールドすべてを調査するアクセスプロファイルを作成します。

```
create access_profile profile_id 1 1 ip source_ip_mask 255.255.255.0
```

上記はスイッチが受信した各フレームの IP フィールドを調査するアクセスプロファイルの例です。スイッチが検出した各送信元 IP アドレスを論理和により source_ip_mask と照合します。profile_id パラメータを使用してアクセスプロファイルに識別番号（ここでは 1）を設定します。スイッチは deny パラメータを使用して規準に合うフレームを廃棄します。（ここでは、次のステップで指定する IP アドレスと ip_source_mask 照合の論理和）。

スイッチのアクセスプロファイルの初期値はトラフィックフローを permit（許可）しています。トラフィックを制限するためには、deny パラメータを使用する必要があります。

アクセスプロファイルの作成後、スイッチがある特定フレームの送信、または廃棄を決定するために基準を追加する必要があります。ここでは、10.42.73.0 と 10.42.73.255 間の IP ソースアドレスを持つすべてのパケットを廃棄するものとします。

```
config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 1 deny
```

ここではアクセスプロファイルの作成時に指定した profile_id 1 を使用しています。「add」パラメータはアクセスプロファイルと関連付けられるルールリストに従う基準をスイッチに追加します。アクセスプロファイルに登録した各ルールに、ルールを識別し、ルールリスト内にプライオリティを設定する access_id を割り当てることができます。数字の小さい access_id ほど高いプライオリティになります。アクセスプロファイルに登録したルール内に矛盾がある場合、最も高いプライオリティ（最も低い access_id）のルールが優先されます。

ip パラメータはこの新しいルールが各フレームヘッダ内の IP アドレスに適用されるようにします。source_ip はこのルールを各フレームヘッダの送信元 IP アドレスに適用するようにスイッチに指示します。最後に、IP アドレス 10.42.73.1 は source_ip_mask 255.255.255.0 に統合し、10.42.73.0 と 10.42.73.255 の間の送信元 IP アドレスに IP アドレス 10.42.73.0 を与えます。

チップセットの制限により最大 14 個のアクセスプロファイルをサポートします。アクセスプロファイルの定義に使用されるルール数は 1 つのスイッチで合計 1792 個です。1 つのルールはポート、またはポートマップごとの ACL をサポートしています。

コマンドラインインタフェース（CLI）におけるアクセスコントロールリストとそのパラメータは以下の通りです。

コマンド	パラメータ
create access_profile	[ethernet{ vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type}| ip { vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code } | igmp {type } | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0 - 0xFF> {user_define_mask <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}]}| ipv6 { class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}|packet_content_mask{offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}][profile_id <value 1-255>]
config access_profile_id	<value 1-255>[add access_id [auto_assign | <value 1-65535>][ethernet { vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> }| ip{ vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> |[icmp {type <value 0-255> code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}]}| ipv6 { class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}|packet_content_mask{offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}]port <portlist>[permit{priority <value 0-7> {replace_priority} | replace_dscp_with <value 0-63> } | deny | mirror] | delete access_id <value 1-65535>]
delete access_profile	[profile_id <value 1-255> | all]
show access_profile	{profile_id <value 1-255> {access_id <value 1-65535>}}
enable cpu_interface_filtering	
disable cpu_interface_filtering	
create cpu access_profile	[ethernet{ vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type}| ip { vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code } | igmp {type } | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0 - 0xFF> {user_define_mask <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}]}|packet_content_mask{offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}][profile_id <value 1-5>]
config cpu access_profile	profile_id <value 1-5>[add access_id <value 1-65535>[ethernet { vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> }| ip{ vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> |[icmp {type <value 0-255> code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}]}|packet_content_mask{offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}][permit | deny] | delete access_id <value 1-65535>]
delete cpu access_profile	profile_id <value 1-5>
show cpu access_profile	{profile_id <value 1-5> {access_id <value 1-65535>}}

以下のセクションで各コマンドについて詳しく記述します。

create access_profile（for Ethernet）

目的

パケットヘッダのイーサネット部分を調査するアクセスプロファイルを作成します。入力するマスクはスイッチが指定したフレームのヘッダフィールドに検出した値に合わせることができます。ルールに対する具体的な値は下の「config access_profile」コマンドを使用します。

構文

create access_profile [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} profile_id <value 1-255>]

説明

このコマンドはパケットヘッダ内のイーサネット部分を調査してスイッチに許可、または拒否されるパケットのプロファイルを作成します。パケットヘッダのイーサネット部分に関連するルールに設定する特定の値は以下に記載されているように「config access_profile」コマンドで定義します。

パラメータ

パラメータ	説明
ethernet	以下のようにスイッチは各パケットヘッダのレイヤ 2 部分を調査します。 • vlan - 各パケットヘッダの VLAN 部分を調査します。 • source_mac <macmask 000000000000-ffffffffffff> - 送信元 MAC アドレスの MAC アドレスマスクを指定します。このマスクは 16 進数（000000000000-FFFFFFFFFFFF）で指定します。 • destination_mac<macmask 000000000000-ffffffffffff> - 送信先 MAC アドレスの MAC アドレスマスクを 16 進数（000000000000-FFFFFFFFFFFF）で指定します。 • 802.1p - フレームヘッダの 802.1p プライオリティ値を調査します。 • ethernet_type - 各フレームヘッダのイーサネットタイプ値を調査します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

イーサネットアクセスプロファイルを作成します。

```
DES-3526:admin#create access_profile ethernet vlan 802.1p profile_id 1
Command: create access_profile ethernet vlan 802.1p profile_id 1
Success.
DES-3526:admin#
```

config access_profile_id（for Ethernet）

目的

本コマンドを使用し、スイッチにイーサネットアクセスプロファイルを設定し、スイッチに使用されるルールに受信パケットを送信するか、廃棄するかを決めるために使用する値を定義します。「create access_profile」コマンドを使用して入力したマスク値は論理和を使用し、指定したフレームのヘッダフィールド内にスイッチが検出した値と統合します。

構文

config access_profile profile_id <value 1-255> [add access_id [auto_assign | <value 1-65535> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} port <port> [permit {priority <value 0-7> {replace_priority} | replace_dscp <value 0-63> } | deny | mirror] delete <value 1-65535>]

説明

各パケットヘッダのイーサネット部分を元にパケットの廃棄または転送のいずれかを行うためにスイッチが使用するルールを定義します。

パラメータ

パラメータ	説明
profile_id <value 1-255>	本コマンドで設定したアクセスプロファイルを識別する番号を 1 から 255 で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。低いプロファイル ID ほどプライオリティが高くなります。
add access_id [auto_assign | <value 1-65535>]	上で指定したアクセスプロファイルにルールを追加します。値は追加ルールの相対的なプライオリティを示します。最大 128 個種類のルールをアクセスプロファイルに設定できます。 • auto_assign - 設定するルールに自動的に 1-65535 の数字を割り当てます。 • <value 1-65535> - 設定するルール ID（1-65535）を指定します。
ethernet	以下のパラメータに基づきパケットの廃棄または送信を決定するために各パケットのレイヤ 2 部分をスイッチが調査します。 • vlan<vlan_name 32> - 既に作成しているこの VLAN だけにアクセスプロファイルを適用します。 • source_mac<macaddr>- 送信元 MAC アドレスを持つパケットだけにアクセスプロファイルを適用します。MAC アドレスエントリは 16 進数（000000000000-FFFFFFFFFFFF）で指定します • destination_mac<macaddr> - 送信先 MAC アドレスを持つパケットだけにアクセスプロファイルを適用します。MAC アドレスエントリは 16 進数（000000000000-FFFFFFFFFFFF）で指定します • 802.1p<value 0-7> - 802.1p プライオリティ値を持つパケットだけにアクセスプロファイルを適用します。 • ethernet_type <hex 0x0-0xffff> - パケットヘッダ内に 16 進数の 802.1Q イーサネットタイプを持つパケットだけにアクセスプロファイルを適用します。
port<portlist>	• <portlist> - イーサネットのアクセスプロファイルをスイッチの各ポートに定義します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）
permit	スイッチによる送信を許可するアクセスプロファイルに適合するパケットを指定します。 • priority <value 0-7> - スイッチに既に設定している 802.1p デフォルトプライオリティを書き換えたい場合に、このパラメータを指定します。パケットが送信される CoS キューを決定するためにこのパラメータを使用します。本フィールドを選択すると、スイッチが受信したパケットの中の、本プライオリティに一致するパケットは、既に指定した CoS キューに送られます。 • {replace_priority} - 指定した CoS キューにパケットを送信する前に、このコマンドで既に指定している基準に適合するパケットの 802.1p デフォルトプライオリティをプライオリティフィールドに入力した値に書き換えたい場合に、このパラメータを入力します。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。
replace_dscp <value 0-63>	コマンドの最初の部分で指定した基準に適合する入力パケットの「DSCP」フィールドに記述される値を指定します。この値はパケットの「DSCP」フィールド内の値を書き換えます。
mirror	アクセスプロファイルに一致するパケットを「config mirror port」コマンドで定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートが設定されている必要があります。
deny	アクセスプロファイルに適合しないパケットはスイッチによって送信することを許可されず破棄されます。
delete access_id <value 1-65535>	イーサネットプロファイルから指定ルールを削除します。最大 65535 個のルールがイーサネットプロファイルに指定できます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

イーサネットプロファイルにルールを指定します。

```
DES-3526:admin#config access profile profile_id 1 add access_id 1 ethernet vlan
Trinity 802.1p 1 port 1 permit priority 1 replace priority
Command: config access profile profile_id 1 add access_id 1 ethernet vlan Trinity
802.1p 1 port 1 permit priority 1 replace priority
Success.
DES-3526:admin#
```

create access_profile（IP）

目的

本コマンドを使用し、パケットヘッダの IP 部分を調査することによりスイッチにアクセスプロファイルを作成します。入力するマスクはスイッチが指定したフレームのヘッダフィールドに検出した値に合わせることができます。ルールに対する具体的な値は下の「config access_profile」コマンドを使用します。

構文

create access_profile ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-xffff>} | protocol_id_mask {user_define_mask <hex 0x0-0xffffffff> <hex 0x0-0xffffffff><hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]} profile_id <value 1-255>}}

説明

パケットヘッダの IP 部分を調査することでスイッチが許可または廃棄するパケットのプロファイルを作成します。パケットヘッダの IP 部分に関連するルールに指定した値は、「config access_profile」コマンドで設定することで定義されます。

パラメータ

パラメータ	説明
ip	以下のパラメータで各パケットの IP フィールドを調査します。 • vlan - 各パケットヘッダの VLAN 部分を調査します。 • source_ip_mask<netmask> - 送信元 IP アドレスの IP アドレスマスクを指定します。 • destination_ip_mask<netmask> - 送信先 IP アドレスの IP アドレスマスクを指定します。 • dscp - 各フレームの Type-of-Service（DiffServ code point、DSCP）フィールドを調査します。 • icmp {type | code} - 各フレームヘッダ内の Internet Control Message Protocol（ICMP）フィールドを調査します。 - type - 各フレームの ICMP Type フィールドを調査します。 - code - 各フレームの ICMP Code フィールドを調査します。 • igmp {type} - 各フレームの Internet Group Management Protocol（IGMP）フィールドを調査します。 - type - 各フレームの IGMP Type フィールドを調査します。 • tcp - 各フレームの Transport Control Protocol（TCP）フィールドを調査します。 - src_port_mask<hex 0x0-0xffff> - 送信元ポートの TCP ポートマスクを指定します。 - dst_port_mask<hex 0x0-0xffff> - 送信先ポートに TCP ポートマスクを指定します。 - flag_mask[all|{urg|ack|psh|rst|syn|fin}]- 対応する flag_mask パラメータを入力します。すべての入力パケットは送信基準として TCP ポート番号を持っており、これらの番号はパケットをどうするかを決定するパケットの一部分に関連する flag bit を持っています。パケット内の特定の flag bit を調査して、パケットを拒否します。次のパラメータから選択できます。all、urg（urgent）、ack（acknowledgement）、psh（push）、rst（reset）、syn（synchronize）、および fin（finish）。 • udp - 各フレームの Universal Datagram Protocol（UDP）フィールドを調査します。 - src_port_mask<hex 0x0-0xffff> - 送信元ポートに UDP ポートマスクを指定します。 - dst_port_mask<hex 0x0-0xffff> - 送信先ポートに UDP ポートマスクを指定します。 • protocol_id_mask - 各フレームのプロトコル ID フィールドを調査します。 - <hex 0x0-0xff>- パケットヘッダ内で検出されるプロトコルを識別する値を 16 進数で指定します。 - user_define_mask <hex 0x0-0xffffffff> - パケットヘッダ内で検出されるユーザ定義のプロトコルを識別する値を 16 進数で指定します。 - profile_id <value 1-255> - このコマンドで作成されるアクセスプロファイルを識別するインデックス番号を 1 から 255 で指定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

IP アクセスプロファイルにルールを設定します。

```
DES-3526:admin#create access_profile ip protocol_id profile_id 2
Command: create access_profile ip protocol_id profile_id 2
Success.
DES-3526:admin#
```

config access_profile（IP）

目的

スイッチに IP アクセスプロファイルを設定し、受信パケットの送信または廃棄を決定するルールに具体的な値を定義します。「create access_profile」コマンドを使用して入力したマスク値は論理和を使用し、指定したフレームのヘッダフィールド内にスイッチが検出した値と統合します。

構文

cconfig access_profile profile_id <value 1-255> [add access_id [auto_assign | <value 1-65535>] ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-255> code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff><hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]} port <port> [permit {priority <value 0-7> {replace_priority} | replace_dscp <value 0-63>} | deny | mirror] delete <value 1-65535>]]

説明

スイッチが使用するルールを定義することで、各パケットヘッダの IP 部分に基づいてパケットを送信またはフィルタします。

パラメータ

パラメータ	説明
profile_id <value 1-255>	本コマンドで設定したアクセスプロファイルを識別する番号を 1 から 255 で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。低いプロファイル ID ほどプライオリティが高くなります。
add access_id [auto_assign | <value 1-65535>	上で指定したアクセスプロファイルにルールを追加します。値は追加ルールの相対的なプライオリティを示します。最大 65535 種類のルールを IP アクセスプロファイルに設定できます。 • auto_assign - 設定するルールに自動的に 1-65535 の数字を割り当てます。 • <value 1-65535> - 設定するルール ID（1-65535）を指定します。
ip	以下のパラメータに基づき廃棄、または送信を決定するために各パケットの IP フィールドを調査します。 • source_ip <ipaddr> - 送信元 IP アドレスを持つパケットだけにアクセスプロファイルを適用する場合に指定します。 • destination_ip <ipaddr> - アクセスプロファイルをこの送信先 IP アドレスを持つパケットにだけ適用します。 • dscp <value 0-63> - アクセスプロファイルを IP パケットヘッダの Type-of-Service（DiffServ code point、DSCP）フィールド内のこの値を持つパケットにだけ適用します。 • icmp - 各パケット内の Internet Control Message Protocol（ICMP）フィールドを調査する場合に指定します。 • igmp - この IGMP タイプを持つパケットにアクセスプロファイルを適用する場合に指定します。 • tcp - 各フレームの Transport Control Protocol（TCP）フィールドを調査します。 - src_port<value 0-65535> - アクセスプロファイルを TCP ヘッダにこの TCP 送信元ポートを持つパケットにだけ適用します。 - dst_port<value 0-65535> - アクセスプロファイルを TCP ヘッダにこの TCP 送信先ポートを持つパケットにだけ適用します。 - urg | ack | psh | rst | syn | fin - マスクする TCP flag のタイプを以下のパラメータより入力します。選択は以下の通りです。 ・ urg:TCP control flag（urgent） ・ ack:TCP control flag（acknowledgement） ・ psh:TCP control flag（push） ・ rst:TCP control flag（reset） ・ fin:TCP control flag（finish） • udp - 各パケットの Universal Datagram Protocol（UDP）フィールドを調査します。 - src_port<value 0-65535> - アクセスプロファイルはヘッダ内に本 UDP 送信元ポートを持つパケットにだけ適用します。 - dst_port<value 0-65535> - アクセスプロファイルはヘッダ内に本 UDP 送信先ポートを持つパケットにだけ適用します。 • protocol_id - 各フレームのプロトコルフィールドを調査します。 - <value 0-255> - フィールドにここで入力した値が含まれていると、適切なルールを適用します。 - user_define<hex 0x0-0xffffffff> - パケットヘッダ内で検出されるユーザ定義のプロトコルを識別する値を 16 進数で指定します。
port<portlist>	• <portlist> - イーサネットのアクセスプロファイルをスイッチの各ポートに定義します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）
permit	スイッチによる送信を許可するアクセスプロファイルに適合するパケットを指定します。 • priority <value 0-7> - スイッチに既に設定している 802.1p デフォルトプライオリティを書き換えたい場合に、このパラメータを指定します。パケットが送信される CoS キューを決定するためにこのパラメータを使用します。本フィールドを選択すると、スイッチが受信したパケットの中の、本プライオリティに一致するパケットは、既に指定した CoS キューに送られます。 • {replace_priority} - 指定した CoS キューにパケットを送信する前に、このコマンドで既に指定している基準に適合するパケットの 802.1p デフォルトプライオリティをプライオリティフィールドに入力した値に書き換えたい場合に、このパラメータを入力します。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。

パラメータ	説明
replace_dscp <value 0-63>	コマンドの最初の部分で指定した基準に適合する入力パケットの「DSCP」フィールドに記述される値を指定します。この値はパケットの「DSCP」フィールド内の値を書き換えます。
mirror	アクセスプロファイルに一致するパケットを「config mirror port」コマンドで定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートが設定されている必要があります。
deny	アクセスプロファイルに適合しないパケットはスイッチによって送信することを許可されず破棄されます。
delete access_id <value 1-65535>	IP プロファイルから指定ルールを削除します。 最大 65535 個のルールが IP プロファイルに指定できます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

IP アクセスプロファイルにルールを設定します。

```
DES-3526:admin#config access_profile profile_id 2 add access_id 2 ip
protocol_id 2 port 1 deny
Command: config access_profile profile_id 2 add access_id 2 ip
protocol_id 2 port 1 deny
Success.
DES-3526:admin#
```

create access_profile（packet content）

目的

本コマンドを使用し、パケットヘッダの内容を調査するアクセスプロファイルを作成します。入力されたパケットコンテンツマスクは、スイッチに識別されるためにパケットヘッダの特定バイトを指定します。設定したオフセットの一つと同一バイトを持つパケットを認識した場合、コマンドに基づいてパケットをフィルタします。ルールに対する具体的な値は下の「config access_profile」コマンドを使用します。

構文

create access_profile packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} profile_id <value 1-255>}

説明

イーサネットパケットヘッダをバイトごとに調査することによってパケットを識別し、ユーザ設定に基づいて、それらをフィルタするか、または送信するかを決定します。「config access_profile」コマンドを使用して 16 進数形式でコマンド内に入力することで、どのバイトを調査するのかを指定し、フィルタまたは送信するのかを選択します。

パラメータ

パラメータ	説明
packet_content_mask	オフセットフィールドは、各ブロックが 4 バイトを表す 4 つの「chunk」に分割されるパケットヘッダを調査するために使用されます。指定されるパケットヘッダブロック内の値は、「mask」フィールドに 16 進数形式で「マスク」フィールドに記載します。 • offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> • offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> • offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> • offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff> 以下のテーブルは、各ブロック内のバイトを指定するための資料です。 chunk0 chunk1 chunk2 …… chunk29 chunk30 chunk31 ===== ===== ===== ====== ====== ====== b126 b2 b6 b114 b118 b122 b127 b3 b7 b115 b119 b123 b1 b4 b8 b116 b120 b124 b0 b5 b9 b117 b121 b125

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

パケットコンテンツマスクによるアクセスプロファイルを作成します。

```
DES-3526:admin#create access_profile packet_content_mask offset_chunk_1 1 0xFFFFFFFF profile_
id 3
Command: create access_profile packet_content_mask offset_chunk_1 1 0xFFFFFFFF profile_id 3

Success.

DES-3526:admin#
```

config access_profile（packet content）

目的

パケットコンテンツマスクに基づき定義済みアクセスプロファイルにルールを設定します。入力されたパケットコンテンツマスクは、スイッチに識別されるためにパケットヘッダの特定バイトを指定します。設定したオフセットの一つと同一バイトを持つパケットを認識した場合、コマンドに基づいてパケットを転送またはフィルタします。

構文

config access_profile profile_id <value 1-8> [add access_id <value 1-65535> packet_content_mask {offset_0-15 <hex0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0- 0xffffffff> <hex 0x0-0xffffffff><hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0- 0xffffffff> <hex0x0-0xffffffff>} port <port> [permit {priority <value 0-7> {replace_priority} | replace_dscp <value 0-63> } | deny | mirror] delete access_id <value 1-65535>]]

説明

本コマンドは、パケットコンテンツマスクに基づいて定義済みアクセスプロファイル設定にルールを設定します。これらのルールは、本コマンドで指定した設定に基づいて確認パケットを転送またはフィルタします。パケットのはじめのバイトからのオフセットを 16 進数形式で入力することで識別するようにバイトを設定します。

パラメータ

パラメータ	説明
profile_id <value 1-255>	アクセスプロファイルを識別する番号を 1 から 255 で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。低いプロファイル ID ほどプライオリティが高くなります。
add access_id [auto_assign | <value 1-65535>	上で指定したアクセスプロファイルにルールを追加します。値は追加ルールの相対的なプライオリティを示します。最大 128 種類のルールを IP アクセスプロファイルに設定できます。 • auto_assign - 設定するルールに自動的に 1-65535 の数字を割り当てます。 • <value 1-65535> - 設定するルール ID（1-65535）を指定します。
port<portlist> | all	• <portlist> - アクセスプロファイルをスイッチの各ポートに定義します。各ポートに最大 128 個まで設定できます。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - すべてのポートを指定します。
permit	スイッチによる送信を許可するアクセスプロファイルに適合するパケットを指定します。 • priority <value 0-7> - スイッチに既に設定している 802.1p デフォルトプライオリティを書き換えたい場合に、このパラメータを指定します。パケットが送信される CoS キューを決定するためにこのパラメータを使用します。本フィールドを選択すると、スイッチが受信したパケットの中の、本プライオリティに一致するパケットは、既に指定した CoS キューに送られます。 • {replace_priority} - 指定した CoS キューにパケットを送信する前に、本コマンドで既に指定している基準に適合するパケットの 802.1p デフォルトプライオリティをプライオリティフィールドに入力した値に書き換える場合に、このパラメータを入力します。指定しない場合は、パケットは送出前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。
mirror	アクセスプロファイルに一致するパケットを「config mirror port」コマンドで定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートが設定されている必要があります。
deny	アクセスプロファイルに適合しないパケットはスイッチによって送信することを許可されず破棄されます。
delete access_id <value 1-65535>	IP プロファイルから指定ルールを削除します。 最大 65535 個のルールが IP プロファイルに指定できます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

パケットコンテンツマスクによるアクセスプロファイルを作成します。

```
DES-3526:admin#config access_profile profile_id 3 add access_id 1 packet_content offset_
chunk_1 0x11111111 port 3 permit priority 2 replace_priority rx_rate no_limit counter enable
Command: config access_profile profile_id 3 add access_id 1 packet_content_mask offset_chunk_1
0x11111111 port 3 permit priority 2 replace_priority rx_rate no_limit counter enable

Success.

DES-3526:admin#
```

create access_profile（ipv6）

目的

本コマンドを使用し、スイッチがパケットヘッダの IPv6 部分を調査するアクセスプロファイルを作成します。マスクを入力し、特定のヘッダフィールド内に検出した値と統合されます。ルールに対する具体的な値は下の「config access_profile」コマンドを使用します。

構文

create access_profile ipv6 profile_id <value 1-8> {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]}

説明

このコマンドはパケットヘッダ内の IPv6 部分を調査してスイッチに許可、または拒否されるパケットのプロファイルを作成します。

パラメータ

パラメータ	説明
profile_id<value 1-8>	このコマンドで作成されるプロファイルを識別するインデックス番号を 1 から 14 で指定します。
ipv6	スイッチは IPv6 の「config access_profile」コマンドで設定したルールに基づき、送信または廃棄するために IPv6 パケットを調査します。IPv6 パケットは以下のパラメータによって識別されます。 • class - このパラメータを入力すると、スイッチは IPv6 ヘッダの class フィールドを調査します。本フィールドは IPv4 における「Type of Service（ToS）」、「Precedence bits」フィールドのようなパケットヘッダの一部です。 • flowlabel - このパラメータを入力すると、スイッチは IPv6 ヘッダの flow label フィールドを調査します。本フィールドは送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではないフィールドです。 • source_ipv6_mask<ipv6mask>- 送信元の IPv6 アドレスの IP アドレスマスクを指定します。 • destination_ipv6_mask<ipv6mask>- 送信先の IPv6 アドレスの IP アドレスマスクを指定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

```
DES-3526:admin#create access_profile profile_id 4 ipv6 class flowlabel
Command: create access_profile profile_id 4 ipv6 class flowlabel

Success.

DES-3526:admin#
```

config access_profile（ipv6）

目的

スイッチに IPv6 アクセスプロファイルの設定を行い、パケットの廃棄または転送を決定するルールにプロファイル値を定義します。

構文

config access_profile profile_id <value 1-8> [add access_id <value 1-65535>] ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destionation_ipv6 <ipv6addr>} port <port> [permit {priority <value 0-7> {replace_priority}} | deny] | delete <value 1-65535>]

説明

各パケットヘッダの IPv6 部分を元にパケットの廃棄または転送を行うためにスイッチが使用するルールを定義します。

パラメータ

パラメータ	説明
profile_id <value 1-8>	このコマンドで作成されるプロファイルを識別するインデックス番号を 1 から 8 で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。低いプロファイル ID ほどプライオリティが高くなります。
add access_id [auto_assign | <value 1-65535>]	上で指定したアクセスプロファイルにルールを追加します。値は追加ルールの相対的なプライオリティを示します。最大 65535 種類のルールを IPv6 アクセスプロファイルに設定できます。 • auto_assign - 設定するルールに自動的に 1-65535 の数字を割り当てます。 • <value 1-65535> - 設定するルール ID（1-65535）を指定します。
ipv6	以下のパラメータに基づいて廃棄、または送信するかを決定するために各パケットの IPv6 フィールドをスイッチが調査します。 • class<value 0-255> - このパラメータを入力すると、スイッチは IPv6 ヘッダの class フィールドを調査します。本フィールドは IPv4 における「Type of Service（ToS）」、「Precedence bits」フィールドのようなパケットヘッダの一部です。 • flowlabel <hex 0x0-fffff> - このパラメータを入力すると、スイッチは IPv6 ヘッダの「flow label」フィールドを調査します。本フィールドは送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではないフィールドです。このフィールドは 16 進数（hex 0x0-0xffff）で定義されます。 • source_ipv6 <ipv6addr> - 送信元 IPv6 アドレスの IP アドレスマスクを指定します。 • destination_ipv6 <ipv6addr> - 送信先 IPv6 アドレスの IP アドレスマスクを指定します。

パラメータ	説明
port<portlist>	• <portlist> - イーサネットのアクセスプロファイルをスイッチの各ポートに定義します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）
permit	スイッチによる送信を許可するアクセスプロファイルに適合するパケットを指定します。 • priority <value 0-7> - スイッチに既に設定した 802.1p デフォルトプライオリティを書き換えたい場合に指定します。本パラメータはパケットが送信される CoS キューを決定します。本フィールドを選択すると、スイッチが受信したパケットの中の、本プライオリティに一致するパケットは、既に指定した CoS キューに送られます。 • {replace_priority} - 指定した CoS キューにパケットを送信する前に、このコマンドで以前指定した、基準に適合するパケットの 802.1p デフォルトプライオリティをプライオリティフィールドに入力した値に書き換えたい場合に、このパラメータを入力します。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。
deny	アクセスプロファイルに適合しないパケットはスイッチによって送信することを許可されず破棄されます。
delete access_id <value 1-65535>	IP プロファイルから指定ルールを削除します。最大 65535 個のルールが IP プロファイルに指定できます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

```
DES-3526:admin#config access_profile profile_id 4 add access_id 1 ipv6 class 1 flowlabel 0xABCD port 1:4
deny
Command: config access_profile profile_id 4 add access_id 1 ipv6 class 1 flowlabel 0xABCD port 1:4 deny

Success.

DES-3526:admin#
```

delete access_profile

目的

作成したアクセスプロファイルを削除します。

構文

delete access_profile [profile_id <value 1-255> | all]

説明

スイッチに作成済みのアクセスプロファイルを削除するために使用されます。

パラメータ

パラメータ	説明
profile_id <value 1-255>	本コマンドで削除するアクセスプロファイルを識別する番号を 1 から 255 で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。
all	IP-MAC バインディングコマンドを使用して自動的に作成したものを除き、スイッチに現在設定されているすべての IP プロファイルを削除します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

プロファイル ID 1 を持つアクセスプロファイルを削除します。

```
DES-3526:admin#delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DES-3526:admin#
```

show access_profile

目的

スイッチに現在設定されているアクセスプロファイルを表示します。

構文

show access_profile {profile_id <value 1-14>}

説明

現在設定されているアクセスプロファイルを表示します。

パラメータ

パラメータ	説明
profile_id<value 1-255>	本コマンドで参照するアクセスプロファイルを識別する番号を 1 から 255 で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。profile_id パラメータなしでコマンドを入力するとすべてのアクセスプロファイルエントリを表示します。

制限事項

なし。

使用例

スイッチに現在設定されているすべてのアクセスプロファイルを表示します。

```
DES-3526:admin#show access_profile
Command: show access_profile

Total Unused Rule Entries : 1791
Total Used Rule Entries   : 1

Access Profile ID:1                                 Type :Packet Contents
===========================================================================
Owner          : ACL
MASK Option    :
offset_chunk_1 : 1           value : 0x11111111

Access ID :3     Mode:Permit(replaced)       Rx Rate(64Kbps): no_limit
                                             (Replaced)Priority: 2

Ports       :8
Time Range  : Tiberius
Total Matched Counter : 0
Offset_chunk_1   : 1   value : 0x11111111
===========================================================================
Unused Entries : 127

DES-3526:admin#
```

enable cpu_interface_filtering

目的

CPU インタフェースフィルタリングを有効にします。

構文

enable cpu_interface_filtering

説明

CPU インタフェースフィルタリングを有効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

CPU インタフェースフィルタリングを有効にします。

```
DES-3526:admin#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DES-3526:admin#
```

disable cpu_interface_filtering

目的

CPU インタフェースフィルタリングを無効にします。

構文

disable cpu_interface_filtering

説明

CPU インタフェースフィルタリングを無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

CPU インタフェースフィルタリングを無効にします。

```
DES-3526:admin#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DES-3526:admin#
```

create cpu access_profile

目的

CPU インタフェースフィルタリングのアクセスプロファイルを特別に作成し、スイッチが調査する入力フレームのヘッダの一部を定義します。マスクを入力し、特定のヘッダフィールド内に検出した値と統合されます。

構文

create cpu access_profile [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0- 0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id {user_mask <hex 0x0- 0xffffffff>}]} | packet_content_mask {offset 0-15 <hex 0x0-0xffffffff> <hex 0x0- 0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>| offset 16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 32-47 <hex 0x0- 0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0- 0xffffffff>}] [profile_id value 1-5>]}

説明

CPU Interface Filtering だけに使用するアクセスプロファイルを作成します。マスクを入力し、特定のヘッダフィールド内に検出した値と統合されます。ルールに対する具体的な値は「config cpu access_profile」コマンドを使用して指定します。

パラメータ

パラメータ	説明
ethernet	各パケットヘッダのレイヤ 2 部分を調査します。 • vlan - 各パケットヘッダの VLAN 部分を調査します。 • source_mac <macmask 000000000000-ffffffffffff> - 送信元 MAC アドレスマスクを調査します。MAC アドレスエントリは 16 進数（000000000000-FFFFFFFFFFFF）で指定します。 • destination_mac <macmask 000000000000-ffffffffffff> - 送信先 MAC アドレスマスクを調査します。MAC アドレスエントリは 16 進数（000000000000-FFFFFFFFFFFF）で指定します。 • ethernet_type - 各フレームヘッダのイーサネットタイプ値を調査します。

パラメータ	説明
ip	各フレームヘッダの IP アドレスを調査します。 • vlan - VLAN マスクを指定します。 • source_ip_mask <netmask>- 送信元 IP アドレスの IP アドレスマスクを指定します。 • destination_ip_mask <netmask>- 送信先 IP アドレスの IP アドレスマスクを指定します。 • dscp - 各フレームヘッダ内の DiffServ Code Point（DSCP）フィールドを調査します。 • icmp - 各フレームヘッダ内の Internet Control Message Protocol（ICMP）フィールドを調査します。 - type - 各フレームの ICMP Type フィールドを調査します。 - code - 各フレームの ICMP Code フィールドを調査します。 • igmp - 各フレームの Internet Group Management Protocol（IGMP）フィールドを調査します。 - type - 各フレームの IGMP Type フィールドを調査します。 • tcp - 各フレームの Transport Control Protocol（TCP）フィールドを調査します。 - src_port_mask <hex 0x0-0xffff> - 送信元ポートの TCP ポートマスクを指定します。 - flag_mask [all| {urg | ack | psh | rst | syn | fin}]- 対応する flag_mask パラメータを入力します。すべての入力パケットは基準を送信するような TCP ポート番号を持っており、これらの番号はパケットをどうするかを決定するパケットの一部分に関連する flag bit を持っています。パケット内の特定の flag bit を調査して、パケットを拒否します。次のパラメータから選択できます。all、urg（urgent）、ack（acknowledgement）、psh（push）、rst（reset）、syn（synchronize）、および fin（finish）。 • udp- 各フレームの Universal Datagram Protocol（UDP）フィールドを調査します。 - src_port_mask <hex 0x0-0xffff> - 送信元ポートに UDP ポートマスクを指定します。 - dst_port_mask <hex 0x0-0xffff> - 送信先ポートに UDP ポートマスクを指定します。 - protocol_id_mask <hex 0x0-0xffffffff> - 各フレームのプロトコル ID フィールドを調査します。16 進数で指定します。 - user_define_mask <hex 0x0-0xffffffff> - IP プロトコル IP と IP ヘッダの後のマスクオプションにルールを適用します。
packet_content_mask	以下の指定したオフセット値で始まるパケットヘッダをマスクします。 • offset_0-15 - 16 進数でパケットの 0 バイト目から 15 バイト目までのマスクを指定します。 • offset_16-31 - 16 進数でパケットの 16 バイト目から 31 バイト目までのマスクを指定します。 • offset_32-47 - 16 進数でパケットの 32 バイト目から 47 バイト目までのマスクを指定します。 • offset_48-63 - 16 進数でパケットの 48 バイト目から 63 バイト目までのマスクを指定します。 • offset_64-79 - 16 進数でパケットの 64 バイト目から 79 バイト目までのマスクを指定します。
ipv6	スイッチは IPv6 の「config cpu access_profile」コマンドで設定したルールに基づき、送信または廃棄するために IPv6 パケットを調査します。 • class<value 0-255> - このパラメータを入力すると、スイッチは IPv6 ヘッダの class フィールドを調査します。本フィールドは IPv4 における「Type of Service（ToS）」、「Precedence bits」フィールドのようなパケットヘッダの一部です。 • flowlabel <hex 0x0-fffff> - このパラメータを入力すると、スイッチは IPv6 ヘッダの「flow label」フィールドを調査します。本フィールドは送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではないフィールドです。このフィールドは 16 進数（hex 0x0-0xffff）で定義されます。 • source_ipv6_mask <ipv6addr> - 送信元 IPv6 アドレスの IP アドレスマスクを指定します。 • destination_ipv6_mask <ipv6addr> - 送信先 IPv6 アドレスの IP アドレスマスクを指定します。
profile_id <value 1-5>	CPU アクセスプロファイルを識別する番号を 1 から 5 で指定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

CPU アクセスプロファイルを作成します。

```
DES-3526:admin#create cpu access_profile profile_id 1 ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code
Command: create cpu access_profile profile_id 1 ip vlan source_ip_mask 20.0.0.0 destination_
ip_mask 10.0.0.0 dscp icmp type code

Success.

DES-3526:admin#
```

config cpu access_profile

目的

CPU インタフェースフィルタリングに使用する CPU アクセスプロファイルを設定し、受信パケットを送信するか、廃棄するかを決めるためにスイッチに使用される特定の値を定義します。「create cpu access_profile」コマンドを使用して入力したマスク値は、論理和を使用して特定のフレームヘッダフィールド内にスイッチが検出した値と統合します。ルールに対する具体的な値は本コマンドを使用して指定します。

構文

config cpu access_profile profile_id <value 1-5>[add access_id <value 1-65535>[ethernet { vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> }| ip{ vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> |[icmp {type <value 0-255> code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}]}|packet_content_mask{offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}][permit | deny] | delete access_id <value 1-65535>]

説明

CPU インタフェースフィルタリングのために CPU アクセスプロファイルを設定し、「create cpu access_profile」コマンドを使用して入力したマスク値と論理和を使用して統合する値を入力します。

パラメータ

パラメータ	説明
profile_id <value 1-5>	本コマンドで設定するアクセスプロファイルを識別する番号を 1 から 5 で指定します。この値はアクセスプロファイルが「create access_profile」コマンドで作成される時に割り当てられます。プロファイル ID はプロファイルに相対的なプロパティを設定し、このコマンドで作成したアクセスプロファイルを識別するインデックス番号を指定します。プライオリティは別のプロファイルとの比較で設定されます。低いプロファイル ID ほどプライオリティが高くなります。
add access_id <value 1-65535>	上で指定したアクセスプロファイルにルールを追加します。値は作成したルールにインデックスをつけるために使用されます。
ethernet	スイッチが各パケットのレイヤ 2 部分だけを調査します。 • vlan <vlan_name 32> - アクセスプロファイルをこの VLAN にだけ適用します。 • source_mac <macaddr 000000000000-ffffffffffff> - アクセスプロファイルをこの送信元 MAC アドレスに適用します。 • destination_mac <macaddr 000000000000-ffffffffffff> - アクセスプロファイルをこの送信先 MAC アドレスにだけ適用します。 • 802.1p <value 0-7> - この 802.1p プライオリティ値を持つパケットだけにアクセスプロファイルを適用します。 • ethernet_type <hex 0x0-0xffff> - パケットヘッダ内に 16 進数の 802.1Q イーサネットタイプを持つパケットだけにアクセスプロファイルを適用します。
ip	各パケットの IP フィールドを調査します。 • vlan <vlan_name 32> - この VLAN だけにアクセスプロファイルを適用します。 • source_ip <ipaddr> - アクセスプロファイルをこの送信元 IP アドレスを持つパケットにだけ適用します。 • destination_ip <ipaddr> - アクセスプロファイルをこの送信先 IP アドレスを持つパケットにだけ適用します。 • dscp <value 0-63> - アクセスプロファイルを IP パケットヘッダの Type-of-Service（DiffServ code point、DSCP）フィールド内のこの値を持つパケットにだけ適用します • icmp - 各パケット内の Internet Control Message Protocol（ICMP）フィールドを調査する場合に指定します。 - type <value 0-255> - アクセスプロファイルを ICMP Type 値に適用します。 - code <value 0-255> - アクセスプロファイルを ICMP Code に適用します。 • igmp - 各パケットの Internet Group Management Protocol（IGMP）フィールドを調査します。 - type <value 0-255> - アクセスプロファイルをこの IGMP type 値を持つパケットに適用します。 • tcp - 各パケットの Transmission Control Protocol（TCP）フィールドを調査します。 - src_port <value 0-65535> - アクセスプロファイルを TCP ヘッダにこの TCP 送信元ポートを持つパケットにだけ適用します。 - dst_port <value 0-65535> - アクセスプロファイルを TCP ヘッダにこの TCP 送信先ポートを持つパケットにだけ適用します。 • udp - 各パケットの Transmission Control Protocol（TCP）フィールドを調査します。 - src_port <value 0-65535> - アクセスプロファイルはヘッダ内にこの UDP 送信元ポートを持つパケットにだけ適用します。 - dst_port <value 0-65535> - アクセスプロファイルはヘッダ内にこの UDP 送信先ポートを持つパケットにだけ適用します。 • protocol_id <value 0-255> - 各パケットのプロトコルフィールドを調査します。このフィールドがここで入力された値を含む場合、以下のルールを適用します。 - user_define <hex 0x0-0xffffffff> - IP プロトコル IP と IP ヘッダの後のマスクオプションにルールを適用します。

パラメータ	説明
packet_content <hex 0x0-0xffffffff>	以下のオフセット値で始まるパケットヘッダをマスクします。 • offset_0-15 - 16 進数でパケットの 0 バイト目から 15 バイト目までのマスクを指定します。 • offset_16-31 - 16 進数でパケットの 16 バイト目から 31 バイト目までのマスクを指定します。 • offset_32-47 - 16 進数でパケットの 32 バイト目から 47 バイト目までのマスクを指定します。 • offset_48-63 - 16 進数でパケットの 48 バイト目から 63 バイト目までのマスクを指定します。 • offset_64-79 - 16 進数でパケットの 64 バイト目から 79 バイト目までのマスクを指定します。
ipv6	以下のパラメータに基づいて廃棄、または送信するかを決定するために各パケットの IPv6 フィールドをスイッチが調査します。 • class<value 0-255> - このパラメータを入力すると、スイッチは IPv6 ヘッダの class フィールドを調査します。本フィールドは IPv4 における「Type of Service（ToS）」、「Precedence bits」フィールドのようなパケットヘッダの一部です。 • flowlabel <hex 0x0-fffff> - このパラメータを入力すると、スイッチは IPv6 ヘッダの「flow label」フィールドを調査します。本フィールドは送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではないフィールドです。このフィールドは 16 進数（hex 0x0-0xffff）で定義されます。 • source_ipv6_mask <ipv6addr> - 送信元 IPv6 アドレスの IP アドレスマスクを指定します。 • destination_ipv6_mask <ipv6addr> - 送信先 IPv6 アドレスの IP アドレスマスクを指定します。
port [<portlist> | all]	• <portlist> - イーサネットのアクセスプロファイルをスイッチの各ポートに定義します。各ポートに最大 128 個まで設定できます。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例: 1:1-1:3,1:7-1:9） • all - すべてのポートを指定します。
permit | deny	このコマンドで設定した基準に適合するパケット CPU へのエントリを許可、または拒否します。
delete access_id <value 1-100>	作成済みの指定プロファイル ID のアクセスルールを削除します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

CPU アクセスリストエントリを設定します。

```
DES-3526:admin#config cpu access_profile profile_id 5 add access_id 1 ip vlan default source_ip
20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1 deny
Command: config cpu access_profile profile_id 10 add access_id 1 ip vlan default source_ip
20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1 deny

Success.

DES-3526:admin#
```

delete cpu access_profile

目的

アクセスプロファイル、または CPU アクセスプロファイルを削除します。

構文

delete cpu access_profile [profile_id <value 1-5>]

説明

作成済みの CPU アクセスプロファイルを削除するために使用されます。

パラメータ

パラメータ	説明
profile_id<value 1-5>	削除する CPU アクセスプロファイルを識別する番号を 1 から 5 で指定します。この値はアクセスプロファイルが「create cpu access_profile」コマンドで作成される時に割り当てられます。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

プロファイル 1 を持つ CPU アクセスプロファイルを削除します。

```
DES-3526:admin#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DES-3526:admin#
```

show cpu access_profile

目的

スイッチに設定されている現在の CPU アクセスプロファイルエントリを参照します。

構文

show cpu access_profile {profile_id <value 1-5> {access_id <value 1-65535>}}

説明

スイッチに設定されている現在の CPU アクセスプロファイルエントリを表示します。

パラメータ

パラメータ	説明
profile_id <value 1-5>	表示するCPUアクセスプロファイルを識別する番号を1から5で指定します。この値はアクセスプロファイルが「create cpu access_profile」コマンドで作成される時に割り当てられます。プロファイル ID パラメータなしでこのコマンドを入力するとすべての CPU アクセスプロファイルエントリを表示します。
access_id <value 1-65535>	表示する CPU アクセスプロファイルを識別する番号を 1 から 65535 で指定します。

制限事項

なし。

使用例

スイッチに設定されている CPU フィルタリングリストを表示します。

```
DES-3526:admin#show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering State:Disabled

CPU Interface Access Profile Table

Access Profile ID:1                                                 Type :Ethernet
================================================================================
MASK Option :
VLAN
----------------------------
Access ID:2     Mode:Permit
Ports:1
----------------------------
default
================================================================================
Total Rule Entries:1

DES-3526:admin#
```

第 25 章　SNTP 設定コマンド

コマンドラインインタフェース（CLI）における SNTP（Simple Network Time Protocol）コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config sntp	{primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}
show sntp	
enable sntp	
disable sntp	
config time	<date ddmthyyyy > <time hh:mm:ss>
config time_zone	{operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
config dst	[disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat>| s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]
show time	

以下のセクションで各コマンドについて詳しく説明します。

config sntp

目的

SNTP サービスを設定します。

構文

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}

説明

SNTP サーバから SNTP サービスを設定します。SNTP を使用するためには、本コマンドにより SNMP を有効にする必要があります（「enable sntp」参照）。

パラメータ

パラメータ	説明
primary<ipaddr>	SNTP 情報を取得するプライマリサーバの IP アドレス。
secondary<ipaddr>	プライマリサーバが使用できない場合に SNTP 情報を取得するセカンダリサーバの IP アドレス。
poll-interval <int 30-99999>	SNTP の更新情報をリクエストする間隔。ポーリング間隔は 30-99999（秒）。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。SNTP を使用するためには、本コマンドにより SNTP を有効にする必要があります（「enable sntp」コマンド参照）。

使用例

SNTP パラメータを設定します。

```
DES-3526:admin#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DES-3526:admin#
```

show sntp

目的

SNTP 情報を表示します。

構文

show sntp

説明

送信元 IP アドレス、時間、およびポーリング間隔を含む SNTP 設定情報を表示します。

パラメータ

なし。

制限事項

なし。

使用例

SNTP 設定情報を表示します。

```
DES-3526:admin#show sntp
Command: show sntp

Current Time Source   :System Clock
SNTP                  :Disabled
SNTP Primary Server   :10.1.1.1
SNTP Secondary Server :10.1.1.2
SNTP poll interval    :720 sec

DES-3526:admin#
```

enable sntp

目的

SNTP サーバサポートを有効にします。

構文

enable sntp

説明

SNTP サポートを有効にします。SNTP サービスは分けて設定する必要があります（「config sntp」コマンド参照）。SNTP サポートを有効にして、設定すると、手動で設定したすべてのシステム時間設定が上書きされます。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。SNTP パラメータは SNTP が機能するように設定される必要があります（「config sntp」コマンド参照）。

使用例

SNTP 機能を有効にします。

```
DES-3526:admin#enable sntp
Command: enable sntp

Success.

DES-3526:admin#
```

disable sntp

目的

SNTP サーバサポートを無効にします。

構文

disable sntp

説明

SNTP サポートを無効にします。SNTP サービスは分けて設定される必要があります（「config sntp」コマンド参照）。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

SNTP を無効にします。

```
DES-3526:admin#disable sntp
Command: disable sntp

Success.

DES-3526:admin#
```

config time

目的

手動でシステム時間と日付の設定を行います。

構文

config time <date ddmthyyyy> <time hh:mm:ss>

説明

システム時間と日付の設定を行います。SNTP が設定され、有効にされると、これらは上書きされます。

パラメータ

パラメータ	説明
date	日付には 2 桁の数字、月には英字 3 文字、年には 4 桁の数字を使用して表します。例 : 03aug2003
time	システム時間は hh:mm:ss 形式で表します（hh: 時、mm: 分、ss: 秒は 2 桁の数字、24 時制）。例 :19:42:30

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。SNTP が有効になると、手動で設定したシステム時間と日付設定は上書きされます。

使用例

システム時間と日付の設定を手動で行います。

```
DES-3526:admin#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DES-3526:admin#
```

config time_zone

目的

使用するタイムゾーンを決定し、システムクロックを調整します。

構文

config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}

説明

タイムゾーンに応じて、システムクロック設定を調整します。そのため、タイムゾーン設定は SNTP 情報を調整します。

パラメータ

パラメータ	説明
operator [+ | -]	グリニッジ標準時に対するタイムゾーンの調整を（+）または（-）でそれぞれ時間をプラスおよびマイナスします。
hour <gmt_hour 0-13>	グリニッジ標準時との差分の時間を指定します。
min <minute 0-59>	プラスまたはマイナスする差分の時間（分）を指定し、タイムゾーンを調整します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

タイムゾーン設定を設定します。

```
DES-3526:admin#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DES-3526:admin#
```

config dst

目的

サマータイム（DST : Savings Time）を有効にし、時間調整を設定します。

構文

config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]

説明

DST を有効にして、設定します。有効にする場合、どの DST 要求にも応じるようにシステムクロックの調整をします。DST 調整は手動による設定した時間および SNTP サービスを利用して設定した時間の両方のシステム時間に作用します。

パラメータ

パラメータ	説明
disable	スイッチの DST 季節時間の調整を無効にします。
repeating	リピートモードを使用すると、DST の季節の時間調整が有効になります。リピートモードでは、DST（サマータイム）の設定を指定する期間が必要となります。例えば、サマータイムを 4 月の第 2 週の土曜日から、10 月の最終週の日曜日までと指定することができます。
annual	アニュアルモードでは、DST の季節の時間調整は有効になります。アニュアルモードでは、DST（サマータイム）の設定を指定する詳細な期日が必要になります。例えば、サマータイムを 4 月 3 日から、10 月 14 日までと指定することができます。
s_week <start_week 1-4,last>	DST が開始する週を設定します。1 は第 1 週目、2 は第 2 週目と続き、last は月の最終週。
e_week <end_week 1-4,last>	DST が終了する週を設定します。1 は第 1 週目、2 は第 2 週目と続き、last は月の最終週。
s_day <start_day sun-sat>	DST が開始する曜日を設定します。3 桁の英字を使用して表された DST が開始する曜日。（sun, mon, tue, wed, thu, fri, sat）
e_day <end_day sun-sat>	DST が終了する曜日を設定します。3 桁の英字を使用して表された DST が終了する曜日。（sun, mon, tue, wed, thu, fri, sat）
s_mth <start_mth 1-12>	DST が開始する月を設定します。
e_mth <end_mth 1-12>	DST が終了する月を設定します。
s_time <start_time hh:mm>	DST が開始する時刻を設定します。24 時制で時刻（hh: 時、mm: 分）を表します。
e_time <end_time hh:mm>	DST が終了する時刻を設定します。24 時制で時刻（hh: 時、mm: 分）を表します。
s_date <start_date 1-31>	DST が開始する特定日（月日）を数字で設定します。
e_date <end_date 1-31>	DST が終了する特定日（月日）を数字で設定します。
offset [30 | 60 | 90 | 120]	サマータイムによる調整時間（プラスまたはマイナス）を指定します。可能なオフセット時間は、30、60、90、120 です。初期値は 60 です。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチにサマータイムを設定します。

```
DES-3526:admin#config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2 e_day wed
e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2 e_day wed e_mth
10 e_time 15:30 offset 30

Success.

DES-3526:admin#
```

show time

目的

現在の時刻設定と状態を表示します。

構文

show time

説明

現在のシステム時間と共に日付と時刻を表示します。

パラメータ

なし。

制限事項

なし。

使用例

現在スイッチに設定されているシステムクロックを表示します。

```
DES-3526:admin#show time
Command: show time

Current Time Source   :System Clock
Boot Time             :23 Aug 2006 09:44:18
Current Time          :23 Aug 2006 15:42:52
Time Zone             :GMT +02:30
Daylight Saving Time  :Repeating
    Offset in minutes :30
    Repeating From    :Apr 2nd Tue 15:00
              To      :Oct 2nd Wed 15:30
       Annual From    :29 Apr 00:00
              To      :12 Oct 00:00

DES-3526:admin#
```

第 26 章　セーフガードエンジンコマンド

ネットワーク上の悪意のあるホストがスイッチに対して、パケットフラッディング（ARP ストーム）などを利用して、周期的に攻撃してくることがあります。これらの攻撃はスイッチに能力以上の負荷を加える可能性があります。このような問題を軽減するために、本スイッチのソフトウェアにセーフガードエンジン機能を付加しました。

セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。スイッチが（a）処理能力を超えた量のパケットを受信した場合、または（b）メモリ使用率が高すぎる場合には、「Exhausted」モードに遷移します。本モードでは、スイッチの稼働を最小化するために、以下のタスクを実行します。

1. 受信 ARP パケットの帯域幅を制限します。「config safeguard_engine」コマンドを使用して 2 つの方法で実行することができます。

- 「strict」を選択すると、スイッチはスイッチに到達しない ARP パケットの受信を中止します。これにより、不必要な ARP パケットをすべて排除し、必要な ARP パケットを不可欠の ARP パケットをスイッチの CPU にパススルーします。

- 「fuzzy」を選択すると、スイッチに到着するかどうかに関わらず、すべての ARP パケットの帯域を調整することによって、スイッチが受信する ARP パケットの帯域を最小化します。スイッチは、内部アルゴリズムを使用し、スイッチに到着する ARP パケットのために確保するように高い割合で ARP パケットをフィルタします。

2. スイッチが受信する IP パケットの帯域幅を制限します。「config safeguard_engine」コマンドを使用して 2 つの方法で実行することができます。

- 「strict」を選択すると、ブロードキャスト IP パケットの高受信レートによって高 CPU 使用率が発生しなくても、スイッチは不必要なブロードキャスト IP パケットの受信を中止します。

- 「fuzzy」を選択すると、IP パケットの帯域の調整、ユニキャストおよびブロードキャスト両方への受信帯域の設定を行うことによって、スイッチが受信する IP パケットの帯域を最小化します。スイッチは、内部アルゴリズムを使用して、ダイナミックに帯域幅を調整中に IP パケットをフィルタします。

また、IP パケットは、受け入れる特定の IP アドレスを設定することで、スイッチに制限されます。前セクションで記述した CPU インタフェースフィルタリングメカニズムを通してこの方式を実行することができます。一度許可する IP アドレスを設定すると、異なる IP アドレスを含む他のパケットは、スイッチに廃棄され、その結果、IP パケットの帯域幅を制限します。処理を高速に保つためには、許可する IP アドレスとそのパケットを受け付ける多くの条件を追加しないように注意してください。多くの条件は CPU の使用率を制限します。

一度セーフガードエンジンは Exhausted モードになると、パケットフローは本モード開始時の半分のレベルまで減少させます。Normal モードに戻ると、パケットを 25% ずつ増加させます。スイッチは、その後間隔をチェックし、スイッチのオーバロードを避けるように動的に通常のパケットフローに戻します。

注意　セーフガードエンジンが有効の場合、本スイッチは FFP（Fast Filter Processor）メータリングテーブルを使用し、各トラフィックフロー（ARP、IP）に帯域を割り当て、CPU 使用率を制御することでトラフィックを制限します。これは、ネットワーク上のトラフィックのルーティング速度を制限します。

コマンドラインインタフェース（CLI）におけるセーフガードエンジンコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config safeguard_engine	{state [enable | disable] | cpu_utilization {rising_threshold <value 20-100> | falling_threshold <value 20-100>} | trap_log [enable | disable]}
show safeguard_engine	

次のセクションで各コマンドについて詳しく説明します。

config safeguard_engine

目的

システムの ARP ストームコントロールを設定します。

構文

config safeguard_engine {state [enable | disable] |cpu_utilization {rising_threshold <value 20-100> | falling_threshold <value 20-100>} |trap_log [enable | disable]}

説明

ARP ストームの影響を最小にするためにセーフガードエンジンを設定します。

パラメータ

パラメータ	説明
state [enable | disable]	セーフガードエンジン機能の実行状態を有効または無効にします。
cpu_utilization	セーフガードエンジン機能のトリガーとなり、以下の実行に基づいて有効になります。 • rising_threshold <value 20-100> - セーフガードエンジン機能のトリガーとなるライジング CPU 使用率の割合を設定します。CPU 使用率がこの割合に上昇するとセーフガードエンジンメカニズムは開始します。 • falling_threshold <value 20-100> - セーフガードエンジン機能のトリガーとなるフォーリング CPU 使用率の割合を設定します。CPU 使用率がこの割合に下がるとセーフガードエンジンメカニズムはシャットダウンします。
trap_log [enable | disable]	セーフガードエンジン機能が CPU 高使用率で作動すると、デバイスの SNMP エージェントとスイッチのログへのメッセージ送信を有効または無効にします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチにセーフガードエンジンエンジンを設定します。

```
DES-3526:admin#config safeguard_engine state enable utilization rising 45
Command: config safeguard_engine state enable utilization rising 45

Success.

DES-3526:admin#
```

show safeguard_engine

目的

現在のセーフガードエンジン設定を表示します。

構文

show safeguard_engine

説明

現在設定されているセーフガードエンジンのステータスとタイプを表示します。

パラメータ

なし。

制限事項

なし。

使用例

セーフガードエンジン状態を表示します。

```
DES-3526:admin#show safeguard_engine
Command: show safeguard_engine

Safeguard Engine State           : Disabled
Safeguard Engine Current Status  : Normal mode
================================================================================
CPU utilization information:
Interval                         : 5 sec
Rising Threshold(20-100)         : 100 %
Falling Threshold(20-100)        : 20 %
Trap/Log                         : Disabled

DES-3526:admin#
```

第 27 章　フィルタコマンド

DHCP Server Screening Setting（DHCP サーバスクリーニング設定）
本機能は、単にすべての DHCP サーバパケットを制限するだけではなく、指定したすべての DHCP クライアントが指定したどんな DHCP サーバパケットに対して受信することも可能とします。そのため、複数の DHCP サーバがネットワークに存在し、異なるクライアントグループに DHCP サービスを提供する場合に役立ちます。DHCP フィルタを有効にすると、ポートごとにアクセスプロファイルとアクセスルールが作成され、以下の示す別のアクセスルールも作成されます。すべての DHCP サーバパケット防御するためにこれらのルールを使用します。同様に、許可する DHCP エントリを追加すると、1 つのアクセスプロファイルを作成し、はじめに 1 つのアクセスルールだけを作成します。この場合、DHCP のクライアントの MAC アドレスは DHCP サーバの IP アドレス（UDP ポート番号 67）と同じです。これらのルールは、ユーザが設定した特定欄を持つ DHCP サーバパケットを許可するために使用されます。

DHCP Client Filtering Setting（DHCP クライアントフィルタリング設定）
指定したサーバの IP アドレスとポートベースで結合するクライアントの MAC アドレスのエントリを作成します。DHCP サーバフィルタ機能を有効にしすべての設定が完了すると、設定されたサーバの IP アドレスとクライアントの MAC アドレスとのバインディングに対応するポートを除き、指定ポートからすべての DHCP サーバパケットをフィルタします。

NetBIOS Filtering Setting（NetBIOS フィルタリング設定）
NetBIOS フィルタ機能を有効にすると、すべての NetBIOS パケットが指定ポートからフィルタされます。NetBIOS フィルタを有効にすると、1 つのアクセスプロファイルが作成されて、ポートごとに 3 つのアクセスルール（UDP ポート番号 137,138、TCP ポート番号 139）が作成されます。「config filter netbios」を有効にすると、802.3 フレームを越えるすべての NetBIOS パケットが指定ポートからフィルタされます。NetBIOS フィルタの状態を設定します。「config filter extensive_netbios」を有効にすると、1 つのアクセスプロファイルが作成されて、ポートごとに 1 つのアクセスルール（DSAP（Destination Service Access Point）=F0 および SASP（Source Service Access Point）=F0）が作成されます。

コマンドラインインタフェース（CLI）における DHCP/NetBIOS フィルタコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config filter dhcp_server	add permit server_ip <ipaddr> client_mac <macaddr> ports [<portlist>|all] | delete permit server_ip <ipaddr> [client_mac <macaddr> | all] | ports [<portlist> | all] state [enable|disable]
show filter dhcp_server	
config filter netbios	<portlist> state [enable|disable]
show filter netbios	
config filter extensive_netbios	<portlist> state [enable|disable]
show filter extensive_netbios	

次のセクションで各コマンドについて詳しく説明します。

config filter dhcp_server

目的

指定の IP アドレス /MAC アドレスから以外の DHCP パケットをフィルタリングします。本コマンドは DHCP パケットフィルタリング機能の有効 / 無効、DHCP サーバ / クライアントエントリの登録 / 消去を設定します。

構文

config filter dhcp_server [add permit server_ip <ipaddr> client_mac <macaddr> ports [<portlist>|all] | delete permit server_ip <ipaddr> [client_mac <macaddr>|all] | ports [<portlist>|all] state [enable|disable]]

説明

本コマンドには 2 つの目的があります。指定のポートからの DHCP パケットをフィルタリングすることと、事前に設定した IP アドレスと MAC アドレスのバインディングリストに対応するの DHCP パケットのみを許可します。この状態は特定の DHCP サーバは指定のクライアントのみに制限された状態でサービスを行うのでネットワーク上に 2 つ以上の DHCP サーバが存在する場合にとても有効です。

パラメータ

パラメータ	説明
add permit server_ip <ipaddr> client_mac <macaddr> ports [<portlist>| all]	add permit server_ip • <lpaddr>- フィルタリングにおいて許可する DHCP サーバの IP アドレスを入力します。 client_mac • <macaddr>- 指定した DHCP サーバと結合するクライアントの MAC アドレスを入力します。 ports • <portlist>- フィルタリングの設定を有効にするポートの名前を入力します。 • all- 全てのポートにおいてフィルタリングの設定を有効にします。
delete permit server_ip <ipaddr>	<lpaddr>- フィルタリングにおい消去する DHCP サーバの IP アドレスを入力します。
client_mac <macaddr>|all	<macaddr>- 指定した DHCP サーバと結合するクライアントの MAC アドレスを消去します。 all - すべてのクライアントの MAC アドレスを消去します。
ports [<portlist>| all]	・<portlist>- 入力したフィルタリングの設定ポートを削除します。 ・all- 全てのフィルタリング設定ポートを削除します。
state [enable| disable]	DHCP フィルタリング機能を有効 / 無効にします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

DHCP フィルタの設定を有効にするとフィルタはアクセスプロファイルと各ポートに対してもアクセスルールを 1 つずつ作成します (UDP port 67) DHCP サーバの追加はエントリに対してアクセスプロファイルとアクセルルールを 1 つずつ作成することを許可します。 (DA = client MAC address, SA = source IP address and UDP port 67).

使用例

スイッチに DHCP フィルタを設定します。

```
DES-3526:admin#config filter dhcp_server add permit_server_ip
10.1.1.1 client_mac 00-00-00-00-00-01 port 1-26
Command: config filter dhcp_server add permit_server_ip 10.1.1.1
client_mac 00-00-00-00-00-01 port 1-26
Success
DES-3526:admin#
```

DHCP フィルタを有効にします。

```
DES-3526:admin#config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable
Success
DES-3526:admin#
```

show filter dhcp_server

目的

スイッチに設定された DHCP サーバ / クライアントフィルタの設定を表示します。

構文

show filter dhcp_server

説明

スイッチに設定された DHCP サーバ / クライアントフィルタの設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

DHCP サーバ / クライアントフィルタリストを表示します。

```
DES-3526:admin#show filter dhcp_server
Command: show filter dhcp_server
Enabled ports: 1-3
Filter DHCP Server/Client Table
Server IP Address Client MAC address Port
------------------------ ---------------------------- --------
10.255.255.254 00-00-00-00-00-01 1-26
DES-3526:admin#
```

DHCP フィルタを有効にします。

```
DES-3526:admin#config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable
Success
DES-3526:admin#
```

config filter netbios

目的

指定のポートからの NetBIOS パケットをフィルタリングします。

構文

config filter netbios <portlist> state [enable|disable]

説明

指定のポートからの NetBIOS パケットをフィルタリングします。

パラメータ

パラメータ	説明
<portlist>	NetBIOS パケットをフィルタリングするポートを入力します。
state [enable|disable]	NetBIOS パケットのフィルタリングを有効 / 無効を設定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

NetBIOS フィルタの有効化によりフィルタはアクセスプロファイル 1 つとアクセスルールを 3 つ各ポートに作成します。(UDP port number 137 and 138, and TCP port 139).

使用例

NetBIOS パケットのフィルタリングを設定します。

```
DES-3526:admin#config filter netbios 1-10 state enable
Command: config filter netbios 1-10 state enable
Success.
DES-3526:admin#
```

show filter netbios

目的

NetBIOS パケットのフィルタリング設定を表示します。

構文

show filter netbios

説明

NetBIOS パケットのフィルタリング設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

NetBIOS パケットのフィルタリング設定を表示します。

```
DES-3526:admin#show filter netbios
Command: show filter netbios
Enabled ports 1-3
DES-3526:admin#
```

config filter extensive_netbios

目的

指定のポートからの 802.3 フレーム NetBIOS パケットのフィルタリングを設定します。

構文

config filter extensive_netbios <portlist> state [enable|disable]

説明

指定のポートからの 802.3 フレーム NetBIOS パケットのフィルタリングを設定します。

パラメータ

パラメータ	説明
<portlist>	NetBIOS パケットをフィルタリングするポートを入力します。
state [enable|disable]	NetBIOS パケットのフィルタリングを有効 / 無効を設定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

NetBIOS フィルタはアクセスプロファイルと各ポートへのアクセスルールを 1 つずつ作成します。(DSAP=F0, SASP=F0).

使用例

extensive NetBIOS パケットのフィルタリングを設定します。

```
DES-3526:admin#config filter extensive_netbios 1-10 state enable
Command: config filter extensive_netbios 1-10 state enable
Success.
DES-3526:admin#
```

show filter extensive_netbios

目的

指定のポートからの 802.3 フレーム NetBIOS パケットのフィルタリング設定を表示します。

構文

show filter extensive_netbios

説明

指定のポートからの 802.3 フレーム NetBIOS パケットのフィルタリング設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

extensive NetBIOS パケットのフィルタリング設定を表示します。

```
DES-3526:admin#show filter extensive_netbios
Command: show filter extensive_netbios
Enabled ports 1-3
DES-3526:admin#
```

第 28 章　トラフィックセグメンテーションコマンド

トラフィックセグメンテーションで、細分化した VLAN をさらに小さいポートグループに分割することで VLAN のトラフィックを軽減します。VLAN ルールが優先され、次に、トラフィックセグメンテーションルールが適用されます。

コマンドラインインタフェース（CLI）におけるトラフィックセグメンテーションコマンドとそのパラメータは以下のとおりです。

コマンド	パラメータ
config traffic_segmentation	[<portlist>] forward_list [null | <portlist>]
show traffic_segmentation	{<portlist>}

以下のセクションで各コマンドについて詳しく説明します。

config traffic_segmentation

目的

スイッチにトラフィックセグメンテーションを設定します。

構文

config traffic_segmentation [<portlist>] forward_list [null | <portlist>]

説明

スイッチにトラフィックセグメンテーションを設定します。

パラメータ

パラメータ	説明
<portlist>	• <portlist> - トラフィックセグメンテーションを設定するポートまたは範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）
forward_list [null | <portlist>]	上で指定されたポートからフレームを受信するポートまたはポート範囲を指定します。 • null - ポートは指定されません。 • <portlist> - フォワーディングリストにポート範囲を指定します。このリストはトラフィックセグメンテーション用に設定されている同じスイッチ上である必要があります。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

管理者レベルまたはオペレータレベルユーザのみ本コマンドを実行できます。

使用例

ポート 6-10 にフレームを転送するためにポート 1-5 を設定します。

```
DES-3526:admin#config traffic_segmentation 1:1-1:5 forward_list 1:6-1:10
Command: config traffic_segmentation 1:1-1:5 forward_list 1:6-1:10

Success.

DES-3526:admin#
```

show traffic_segmentation

目的

スイッチで使用中の現在のトラフィックセグメンテーション設定を表示します。

構文

show traffic_segmentation {<portlist>}

説明

スイッチの現在のトラフィックセグメンテーション設定を表示します。

パラメータ

パラメータ	説明
<portlist>	スイッチの現在のトラフィックセグメンテーションを表示するポートまたはポート範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9）

制限事項

セグメンテーションのポートリストおよびフォワーディングリストは、同じスイッチにある必要があります。

使用例

現在のトラフィックセグメンテーション設定を表示します。

```
DES-3526:admin#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port    Forward Portlist
------  -------------------------------------------------
1       1-26
2       1-26
3       1-26
4       1-26
5       1-26
6       1-26
7       1-26
8       1-26
9       1-26
10      1-26
11      1-26
12      1-26
13      1-26
14      1-26
15      1-26
16      1-26
17      1-26
18      1-26
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

第 29 章　ARP コマンド

コマンドラインインタフェース（CLI）における ARP コマンドとそのパラメータは以下のです。

コマンド	パラメータ
create arpentry	<ipaddr> <macaddr>
config arpentry	<ipaddr> <macaddr>
delete arpentry	{[<ipaddr> | all]}
show arpentry	{ipif <ipif_name 12> | ipaddress <ipaddr> | [static | local]}
config arp_aging time	<value 0-65535>
clear arptable	

以下のセクションで各コマンドについて詳しく説明します。

create arpentry

目的

ARP テーブルにスタティックエントリを作成します。

構文

create arpentry <ipaddr> <macaddr>

説明

スイッチの ARP テーブルに IP アドレスと対応する MAC アドレスを入力します。

パラメータ

パラメータ	説明
<ipaddr>	エンドノードまたはステーションの IP アドレス。
<macaddr>	上記 IP アドレスに対応する MAC アドレス。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。本スイッチは、255 個のスタティック ARP エントリをサポートしています。

使用例

IP アドレス 10.48.74.121 と MAC アドレス「00:50:BA:00:07:36」というスタティック ARP エントリ作成します。

```
DES-3526:admin#create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DES-3526:admin#
```

config arpentry

目的

ARP テーブルのスタティック ARP エントリを設定します。

構文

config arpentry <ipaddr> <macaddr>

説明

ARP テーブルにスタティックエントリを設定します。スイッチの ARP テーブルにエントリの IP アドレスと対応する MAC アドレスを入力します。

パラメータ

パラメータ	説明
<ipaddr>	エンドノードまたはステーションの IP アドレス。
<macaddr>	上記 IP アドレスに対応する MAC アドレス。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

IP アドレス 10.48.74.12 と MAC アドレス 00:50:BA:00:07:36 というスタティック ARP エントリを設定します。

```
DES-3526:admin#config arpentry 10.48.74.12 00-50-BA-00-07-36
Command: config arpentry 10.48.74.12 00-50-BA-00-07-36

Success.

DES-3526:admin#
```

delete arpentry

目的

ARP テーブルのスタティック ARP エントリを削除します。

構文

delete arpentry {[<ipaddr> | all]}

説明

上記「create arpentry」コマンドで作成したスタティック ARP エントリを、エントリの IP アドレスまたは「all」を指定することにより削除します。「all」を指定すると、スイッチの ARP テーブルはクリアされます。

パラメータ

パラメータ	説明
<ipaddr>	エンドノードまたはステーションの IP アドレス。
all	スタティック ARP エントリを削除します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

IP アドレス「10.48.74.121」を持つエントリを ARP テーブルから削除します。

```
DES-3526:admin#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DES-3526:admin#
```

show arpentry

目的

ARP テーブルを表示します。

構文

show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | [static | local]}

説明

スイッチの ARP テーブルにおける現在の内容を表示します。

パラメータ	説明
ipif <ipif_name 12>	作成された ARP テーブルのエンドノードまたはステーションが存在する IP インタフェース名。
ipaddress <ipaddr>	上記 IP インタフェースに対応するネットワークアドレス。
[static | local]	static - ARP テーブル内のスタティックエントリを表示します。 local - ARP テーブル内のローカルエントリを表示します。

制限事項

なし。

使用例

ARP テーブルを表示します。

```
DES-3526:admin#show arpentry
Command: show arpentry

ARP Aging Time :30

Interface IP Address     MAC Address       Type
--------- -------------  ----------------- --------------
System    10.0.0.0       FF-FF-FF-FF-FF-FF Local/Broadcast
System    10.1.1.169     00-50-BA-70-E4-4E Dynamic
System    10.1.1.254     00-01-30-FA-5F-00 Dynamic
System    10.9.68.1      00-A0-C9-A4-22-5B Dynamic
System    10.9.68.4      00-80-C8-2E-C7-45 Dynamic
System    10.10.27.51    00-80-C8-48-DF-AB Dynamic
System    10.11.22.145   00-80-C8-93-05-6B Dynamic
System    10.11.94.10    00-10-83-F9-37-6E Dynamic
System    10.14.82.24    00-50-BA-90-37-10 Dynamic
System    10.15.1.60     00-80-C8-17-42-55 Dynamic
System    10.17.42.153   00-80-C8-4D-4E-0A Dynamic
System    10.19.72.100   00-50-BA-38-7D-5E Dynamic
System    10.21.32.203   00-80-C8-40-C1-06 Dynamic
System    10.40.44.60    00-50-BA-6B-2A-1E Dynamic
System    10.42.73.221   00-01-02-03-04-00 Dynamic
System    10.44.67.1     00-50-BA-DA-02-51 Dynamic
System    10.47.65.25    00-50-BA-DA-03-2B Dynamic
System    10.50.8.7      00-E0-18-45-C7-28 Dynamic
System    10.90.90.90    00-01-02-03-04-00 Local
System    10.255.255.255 FF-FF-FF-FF-FF-FF Local/Broadcast

Total Entries : 20

DES-3526:admin#
```

config arp_aging time

目的

スイッチの ARP テーブルエントリにエージングタイマを設定します。

構文

config arp_aging time <value 0-65535>

説明

テーブルから削除される前に ARP エントリがアクセスされないまま、スイッチの ARP テーブルに保存される最大時間（秒）を設定します。

パラメータ

パラメータ	説明
time <value 0-65535>	ARP エージングタイム（秒）。値は 0-65535 の範囲から指定できます。初期値は 20（秒）です。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

ARP エージングタイムを設定します。

```
DES-3526:admin#config arp_aging time 30
Command: config arp_aging time 30

Success.

DES-3526:admin#
```

clear arptable

目的

すべてのダイナミック ARP テーブルエントリを削除します。

構文

clear arptable

説明

スイッチの ARP テーブルからダイナミック ARP テーブルエントリを削除します。スタティック ARP テーブルエントリは影響を受けません。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

ARP テーブル内のダイナミックエントリを削除します。

```
DES-3526:admin#clear arptable
Command: clear arptable

Success.

DES-3526:admin#
```

第 30 章　ルーティングテーブルコマンド

コマンドラインインタフェース（CLI）におけるルーティングテーブルコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
create iproute	[default] <ipaddr> {<metric 1-65535>}
delete iproute	[default]
show iproute	

以下のセクションで各コマンドについて詳しく説明します。

create iproute

目的

スイッチの IP ルーティングテーブルに IP ルートエントリを作成します。

構文

create iproute [default] <ipaddr> {<metric 1-65535>}

説明

IP ルートエントリをスイッチの IP ルーティングテーブルにします。本ルートには、プライマリ、バックアップまたは重み付けマルチパスがあります。

パラメータ

パラメータ	説明
default	デフォルトのスタティック IP ルートエントリをスイッチの IP ルーティングテーブルに作成するのに使用します。
<ipaddr>	ネクストホップルータのゲートウェイの IP アドレス。
<metric 1-65535>	ルーティングプロトコルのメトリック値。スイッチと上記 IP アドレス間のルータの数を表します。初期値は 1（秒）です

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スタティックアドレス「10.48.74.121」、マスク「255.0.0.0」、およびゲートウェイ「10.1.1.254」をルーティングテーブルに追加します。

```
DES-3526:admin#create iproute 10.48.74.121/255.0.0.0 10.1.1.254 1
Command: create iproute 10.48.74.121/8 10.1.1.254 1

Success.

DES-3526:admin#
```

delete iproute

目的

スイッチの IP ルーティングテーブルから IP ルートエントリを削除します。

構文

delete iproute [default]

説明

スイッチの IP ルーティングテーブルから既存のエントリを削除します。

パラメータ

パラメータ	説明
default	スイッチの IP ルーティングテーブルからデフォルトのスタティック IP ルートエントリを削除します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スタティックアドレス「10.48.74.121」、マスク「255.0.0.0」、およびゲートウェイ「10.1.1.254」をルーティングテーブルから削除します。

```
DES-3526:admin#delete iproute 10.48.74.121/8 10.1.1.254
Command: delete iproute 10.48.74.121/8 10.1.1.254

Success.

DES-3526:admin#
```

show iproute

目的

スイッチの現在の IP ルーティングテーブルを表示します。

構文

show iproute

説明

スイッチの現在の IP ルーティングテーブルを表示します。

パラメータ

なし。

制限事項

なし。

使用例

IP ルーティングテーブルの内容を表示します。

```
DES-3526:admin#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway   Interface    Cost       Protocol
------------------  -------   ---------    -------    --------
10.0.0.0/8          0.0.0.0   System       1          Local

Total Entries : 1

DES-3526:admin#
```

第 31 章　MAC 通知コマンド

コマンドラインインタフェース（CLI）における MAC 通知コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable mac_notification	
disable mac_notification	
config mac_notification	{interval <int 1-2147483647> | historysize <int 1-500>}
config mac_notification ports	[<portlist> | all] [enable | disable]
show mac_notification	
show mac_notification ports	{<portlist>}

以下のセクションで各コマンドについて詳しく説明します。

enable mac_notification

目的

スイッチでグローバルな MAC アドレステーブル通知を有効にします。

構文

enable mac_notification

説明

設定変更しないで、MAC アドレス通知を有効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

基本設定を変更しないで、MAC 通知を有効にします。

```
DES-3526:admin#enable mac_notification
Command: enable mac_notification

Success.

DES-3526:admin#
```

disable mac_notification

目的

スイッチでグローバルな MAC アドレステーブル通知を無効にします。

構文

disable mac_notification

説明

設定変更しないで、MAC アドレス通知を無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

基本設定を変更しないで、MAC 通知を無効にします。

```
DES-3526:admin#disable mac_notification
Command: disable mac_notification

Success.

DES-3526:admin#
```

config mac_notification

目的

MAC アドレス通知を設定します。

構文

config mac_notification {interval <int 1-2147483647> | historysize <int 1-500>}

説明

MAC アドレス通知は、学習され、FDB に入力された MAC アドレスをモニタします。

パラメータ

パラメータ	説明
interval <int 1-2147483647>	通知間隔（秒）。間隔は 1-2147483647（秒）から選択します。
historysize <int 1-500>	通知に使用されるヒストリログに一覧表示されるエントリの最大数。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチの MAC アドレステーブル通知のグローバルパラメータを設定します。

```
DES-3526:admin#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DES-3526:admin#
```

config mac_notification ports

目的

MAC アドレス通知状態を設定します。

構文

config mac_notification ports [<portlist | all] [enable | disable]

説明

MAC アドレス通知は、学習されて FDB に入力された MAC アドレスをモニタします。

パラメータ

パラメータ	説明
<portlist> | all	• <portlist> - 設定するポートまたはポート範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） • all - システムのすべてのポートを設定します。
enable | disable	MAC アドレス通知状態を「enable」（有効）または「disable」（無効）にします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

ポート 7 の MAC アドレステーブル通知を有効にします。

```
DES-3526:admin#config mac_notification ports 1:7 enable
Command: config mac_notification ports 1:7 enable

Success.

DES-3526:admin#
```

show mac_notification

目的
スイッチの MAC アドレステーブル通知のグローバルパラメータを表示します。
構文
show mac_notification
説明
スイッチの MAC アドレステーブル通知のグローバルパラメータを表示します。
パラメータ
なし。
制限事項
なし。
使用例
MAC アドレステーブル通知のグローバル設定を表示します。

```
DES-3526:admin#show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State        :Enabled
Interval     :1
History Size :500

DES-3526:admin#
```

show mac_notification ports

目的
スイッチの MAC アドレステーブル通知の状態を参照します。
構文
show mac_notification ports {<portlist>}
説明
スイッチの MAC アドレステーブル通知の状態設定を表示します。
パラメータ

パラメータ	説明
<portlist>	参照するポートまたはポート範囲を指定します。ポートリストは、「:」（コロン）で分け、スイッチ番号と開始番号の一覧で指定されます。ポートの範囲は、「-」（ダッシュ）を使用して指定します。続き番号ではないポートリストエントリは「,」（カンマ）で分けます。（例 : 1:1-1:3,1:7-1:9） パラメータなしでこのコマンドを入力すると、全ポートに対する MAC 通知テーブルを表示します。

制限事項
なし
使用例
すべての MAC アドレステーブル通知の状態設定を表示します。

```
DES-3526:admin#show mac_notification ports
Command: show mac_notification ports

Port #  MAC Address Table Notification State
------  ------------------------------------
1                   Disabled
2                   Disabled
3                   Disabled
4                   Disabled
5                   Disabled
6                   Disabled
7                   Disabled
8                   Disabled
9                   Disabled
10                  Disabled
11                  Disabled
12                  Disabled
13                  Disabled
14                  Disabled
15                  Disabled
16                  Disabled
17                  Disabled
18                  Disabled
19                  Disabled
20                  Disabled
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

第 32 章　アクセス認証コントロールコマンド

TACACS/ XTACACS/ TACACS+/ RADIUS コマンドは、TACACS/ XTACACS/ TACACS+ /RADIUS プロトコルを使用してスイッチへの安全なアクセスを可能にします。ユーザがスイッチへのログインや、管理者レベルの特権へのアクセスを行おうとする時、パスワードの入力を求められます。TACACS/ XTACACS/ TACACS+/ RADIUS 認証がスイッチで有効になると、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバと連絡し、ユーザの確認をします。確認が行われたユーザは、スイッチへのアクセスを許可されます。

現在 TACACS セキュリティプロトコルには異なるエンティティを持つ 3 つのバージョンが存在します。本スイッチのソフトウェアは TACACS の以下のバージョンをサポートします。

•TACACS（Terminal Access Controller Access Control System）
　セキュリティのためのパスワードチェック、認証、およびユーザアクションの通知を、1 台またはそれ以上の集中型の TACACS サーバを使用して行います。パケットの送受信には UDP プロトコルを使用します。
• XTACACS（拡張型 TACACS）
　TACACS プロトコルの拡張版で、TACACS プロトコルより多種類の認証リクエストとレスポンスコードに対応します。パケットの送受信に UDP プロトコルを使用します。
• TACACS+（Terminal Access Controller Access Control System plus）
　ネットワークデバイスの認証のために詳細なアクセス制御を提供します。TACACS+ は、1 台またはそれ以上の集中型のサーバを経由して認証コマンドを使用することができます。TACACS+ プロトコルは、スイッチと TACACS+ デーモンの間のすべてのトラフィックを暗号化します。また、TCP プロトコルを使用して信頼性の高い伝達を行います。

TACACS/ XTACACS/ TACACS+/ RADIUS のセキュリティ機能が正常に動作するためには、スイッチ以外の認証サーバホストと呼ばれるデバイス上で認証用のユーザ名とパスワードを含む TACACS/ XTACACS/ TACACS+/ RADIUS サーバの設定を行う必要があります。スイッチがユーザにユーザ名とパスワードの要求を行う時、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバにユーザ認証の問い合わせを行います。サーバは以下の 3 つのうちの 1 つの応答を返します。

• サーバは、ユーザ名とパスワードを認証し、ユーザにスイッチへの通常のアクセス権を与えます。
• サーバは、入力されたユーザ名とパスワードを受け付けず、スイッチへのアクセスを拒否します。
• サーバは、認証の問い合わせに応じません。この時点でスイッチはサーバからタイムアウトを受け取り、メソッドリスト中に設定された次の認証方法へと移行します。

本スイッチには TACACS、XTACACS、TACACS+、RADIUS の各プロトコル用に 4 つの認証サーバグループがあらかじめ組み込まれています。これらの認証サーバグループはスイッチにアクセスを試みるユーザの認証に使用されます。認証サーバグループ内に任意の順番で認証サーバホストを設定し、ユーザがスイッチへのアクセス権を取得する場合、1 番目の認証サーバホストに認証を依頼します。認証が行われなければ、リストの 2 番目のサーバホストに依頼し、以下同様の処理が続きます。実装されている認証サーバグループには、特定のプロトコルが動作するホストのみを登録できます。例えば TACACS 認証サーバグループは、TACACS 認証サーバホストのみを登録できます。

スイッチの管理者は、ユーザ定義のメソッドリストに 6 種類の異なる認証方法（TACACS/ XTACACS/ TACACS+/ RADIUS/ local/ none）を設定できます。これらの方法は、任意に並べ替えることが可能で、スイッチ上での通常のユーザ認証に使用されます。リストには最大 8 つの認証方法を登録できます。ユーザがスイッチにアクセスしようとすると、スイッチはリストの 1 番目の認証方法を選択して認証を行います。1 番目の方法で認証サーバホストを通過しても認証が返ってこなければ、スイッチはリストの次の方法を試みます。この手順は、認証が成功するか、拒否されるか、またはリストのすべての認証方法を試し終わるまで繰り返されます。

スイッチへのアクセス権を取得したユーザは、通常のアクセス権を与えられていることにご注意ください。管理者特権レベルの権利を取得するためには、ユーザは「enable admin」コマンドにアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。

注意　TACACS、XTACACS、TACACS+、RADIUS は独立したエンティティであり、互換性はありません。スイッチとサーバ間は、同じプロトコルを使用した全く同じ設定を行う必要があります。（例えば、スイッチに TACACS 認証を設定した場合、ホストサーバにも同様の設定を行います。）

コマンドラインインタフェース（CLI）におけるアクセス認証コントロールコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable authen_policy	
disable authen_policy	
show authen_policy	
create authen_login method_list_name	<string 15>
config authen_login	[default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}
delete authen_login method_list_name	<string 15>
show authen_login	{default | method_list_name <string 15> | all}
create authen_enable method_list_name	<string 15>
config authen_enable	[default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}
delete authen_enable method_list_name	<string 15>
show authen_enable	[default | method_list_name <string 15> | all]
config authen application	{console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]
show authen application	
create authen server_group	<string 15>
config authen server_group	[tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
delete authen server_group	<string 15>
show authen server_group	<string 15>
create authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
config authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
delete authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
show authen server_host	
config authen parameter response_timeout	<int 0-255>
config authen parameter attempt	<int 1-255>
show authen parameter	
enable admin	
config admin local_enable	

以下のセクションで各コマンドについて詳しく説明します。

enable authen_policy

目的

システムアクセス認証ポリシーを有効にします。

構文

enable authen_policy

説明

本メニューは、管理者が定義するスイッチにアクセスするユーザのための認証ポリシーを有効にするために使用します。有効にすると、デバイスはログインメソッドリストをチェックし、ログイン時のユーザ認証に使用する認証方法を選択します。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

システムアクセス認証ポリシーを有効にします。

```
DES-3526:admin#enable authen_policy
Command: enable authen_policy

Success.

DES-3526:admin#
```

disable authen_policy

目的
システムアクセス認証ポリシーを無効にします。
構文
disable authen_policy
説明
管理者が定義するスイッチにアクセスするユーザのための認証ポリシーを無効にします。無効になると、スイッチはユーザ名とパスワード検証のためにローカルユーザアカウントデータベースにアクセスします。さらに、スイッチは、現在、管理者レベルの権限にアクセスを試みる普通のユーザのために認証として「local enable password」を受け付けます。
パラメータ
なし。
制限事項
管理者レベルユーザのみ本コマンドを実行できます。
使用例
システムアクセス認証ポリシーを無効にします。

```
DES-3526:admin#disable authen_policy
Command: disable authen_policy

Success.

DES-3526:admin#
```

show authen_policy

目的
スイッチのシステムアクセス認証ポリシー状態を表示します。
構文
show authen_policy
説明
スイッチにおけるアクセス認証ポリシーの現在のステータスを表示します。
パラメータ
なし。
制限事項
なし。
使用例
システムアクセス認証ポリシーを表示します。

```
DES-3526:admin#show authen_policy
Command: show authen_policy

Authentication Policy:Enabled

DES-3526:admin#
```

create authen_login method_list_name

目的
ユーザがスイッチにログインする際の認証方法を規定するユーザ定義のログインメソッドリストを作成します。
構文
create authen_login method_list_name <string 15>
説明
ユーザログイン用の認証方法のリストを作成します。本スイッチは、最大 8 個のメソッドリストをサポートしていますが、1 つはデフォルトとして予約されているため、削除できません。複数のメソッドリストは、別々に作成および設定される必要があります。
パラメータ

パラメータ	説明
method_list_name <string 15>	15 文字以内の半角英数字の文字列を入力して、メソッドリストを定義します。

制限事項
管理者レベルユーザのみ本コマンドを実行できます。
使用例
メソッドリスト「DLee」を作成します。

```
DES-3526:admin#create authen_login method_list_name DLee
Command: create authen_login method_list_name DLee

Success.

DES-3526:admin#
```

config authen_login

目的

ユーザがスイッチにログインする際の認証方法を規定するユーザ定義またはデフォルトのメソッドリストを設定します。

構文

config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}

説明

本コマンドでは、ユーザがスイッチにログインする際の認証方法を規定するユーザ定義または初期設定のログインメソッドリストを設定します。本メニューで設定した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに TACACS - XTACACS - Local の順番で認証方法を指定すると、スイッチはまずサーバグループ内の 1 番目の TACACS ホストに認証リクエストを送信します。そのサーバホストから応答がない場合、2 番目の TACACS ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリストの次の方法（XTACACS）を試します。それでも認証が行われなければ、スイッチ内に設定したローカルアカウントデータベースを使用して認証を行います。Local メソッドが使用される時、ユーザの権限はスイッチに設定されたローカルアカウントの権限に依存します。

これらの方法によって、認証に成功したユーザには「User」の権限のみが与えられます。ユーザが管理者レベルの権限に更新したい場合、「enable admin」コマンドを実行し、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。（詳細については、「enable admin」の説明を参照してください。）

パラメータ

パラメータ	説明
default | method_list_name <string 15>	• default - ユーザに定義されたアクセス認証のためのデフォルトメソッドリスト。 • method_list_name <string 15> - ユーザによって定義されたメソッドリスト名を入力します。本メソッドリストに追加する認証方法を最大 4 件まで指定します。
method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}	• tacacs - リモートの TACACS サーバから TACACS プロトコルを使用してユーザ認証を行います。 • xtacacs - リモートの XTACACS サーバから XTACACS プロトコルを使用してユーザ認証を行います。 • tacacs+ - リモートの TACACS+ サーバから TACACS+ プロトコルを使用してユーザ認証を行います。 • radius - リモートの RADIUS サーバから RADIUS プロトコルを使用してユーザ認証を行います。 • server_group <string 15> - スイッチに設定したユーザ定義のサーバグループを使用してユーザ認証を行います。 • local - スイッチ上のローカルユーザアカウントデータベースを使用してユーザ認証を行います。 • none - スイッチへアクセスするために認証要求はしません。

注意 認証プロトコルとして「none」または「local」を入力すると、メソッドリストまたはデフォルトメソッドリストに別の認証が上書きされます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

認証メソッド tacacs、xtacacs および local をこの順番でユーザ定義メソッドリスト「DLee」に設定します。

```
DES-3526:admin#config authen_login method_list_name DLee method tacacs xtacacs local
Command: config authen_login method_list_name DLee method tacacs xtacacs local

Success.

DES-3526:admin#
```

使用例

認証メソッド xtacacs、tacacs+ および local をこの順番でデフォルトのメソッドリストに設定します。

```
DES-3526:admin#config authen_login default method xtacacs tacacs+ local
Command: config authen_login default method xtacacs tacacs+ local

Success.

DES-3526:admin#
```

delete authen_login method_list_name

目的

ユーザがスイッチにログインする際の認証方法を規定するユーザ定義のログインメソッドリストを削除します。

構文

delete authen_login method_list_name <string 15>

説明

ユーザログイン用の認証方法のリストを削除します。

パラメータ

パラメータ	説明
method_list_name <string 15>	15 文字以内の半角英数字の文字列を入力して、メソッドリストを削除します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

メソッドリスト「DLee」を削除します。

```
DES-3526:admin#delete authen_login method_list_name DLee
Command: delete authen_login method_list_name DLee

Success.

DES-3526:admin#
```

show authen_login

目的

ユーザがスイッチにログインする際の認証方法を規定するユーザ定義のログインメソッドリストを表示します。

構文

show authen_login [default | method_list_name <string 15> | all]

説明

ユーザがスイッチにログインする際の認証方法を参照します。

パラメータ

パラメータ	説明
default	ユーザがスイッチにログインする際の認証方法を規定するデフォルトのメソッドリストを表示します。
method_list_name <string 15>	15 文字以内の半角英数字の文字列で、参照するメソッドリストを入力します。
all	現在スイッチに設定されているすべての認証ログインメソッドを表示します。

画面には以下のパラメータが表示されます。

パラメータ	説明
Method List Name	設定されているメソッドリスト名。
Priority	ユーザがスイッチにログインする場合、認証のために問い合わせされるメソッドリストプロトコルの順番を定義します。優先順位は 1（最も高い）から 4（最も低い）です。
Method Name	メソッドリスト名ごとに実行されるセキュリティプロトコルを定義します。
Comment	メソッドのタイプを定義します。ユーザ定義のグループは、ユーザが定義したサーバグループを参照します。実装されているグループは、スイッチ内の普遍設定である TACACS、XTACACS、TACACS+ および RADIUS セキュリティプロトコルを参照します。キーワードは「local」（スイッチのユーザアカウント経由の認証）と「none」（スイッチのすべての機能にアクセスするために認証は必要なし）という TACACS/XTACACS/TACACS+/RADIUS の代わりの技術を使用して認証を参照します。

制限事項

なし。

使用例

「Trinity」という認証ログインメソッドリストを参照します。

```
DES-3526:admin#show authen_login method_list_name Trinity
Command: show authen_login method_list_name Trinity

Method List Name Priority Method Name   Comment
---------------- -------- ----------- ---------------
Trinity           1       tacacs+     Built-in Group
                  2       tacacs      Built-in Group
                  3       ctsnow      User-defined Group
                  4       local       Keyword


DES-3526:admin#
```

create authen_enable method_list_name

目的

ノーマルユーザ権限を管理者権限に昇格するための認証方法を規定するユーザ定義のログインメソッドリストを作成します。

構文

create authen_enable method_list_name <string 15>

説明

スイッチで認証メソッドを使用して、ユーザの権限をユーザレベルから管理者（Admin）レベルに上げます。通常のユーザレベルの権限を取得したユーザが管理者特権を得るためには、管理者が定義した方法により認証を受ける必要があります。最大 8 件の Enable Method List がスイッチで実行されます。

パラメータ

パラメータ	説明
method_list_name <string 15>	15 文字以内の半角英数字の文字列を入力して、enable メソッドリストを作成します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ユーザ権限を管理者権限に昇格するために「Permit」という名のユーザ定義メソッドリストを作成します。

```
DES-3526:admin#create authen_enable method_list_name Permit
Command: show authen_login method_list_name Permit

Success.

DES-3526:admin#
```

config authen_enable

目的

スイッチでユーザの権限をユーザレベルから管理者（Admin）レベルに上げる認証メソッドのユーザ定義メソッドリストを設定します。

構文

config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}

説明

スイッチで認証メソッドを使用して、ユーザの権限をユーザレベルから管理者（Admin）レベルに上げます。通常のユーザレベルの権限を取得したユーザが管理者特権を得るためには、管理者が定義した方法により認証を受ける必要があります。最大 8 件の Enable Method List が登録できます。

本コマンドで設定した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに tacacs-xtacacs-local_enable の順番で認証方法を指定すると、スイッチはまずサーバグループ内の 1 番目の tacacs ホストに認証リクエストを送信します。そのサーバホストから応答がない場合、2 番目の tacacs ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリストの次の方法（xtacacs）を試します。それでも認証が行われなければ、スイッチ内に設定し「local_enable password」を使用して認証を行います。

これらの中のひとつの方法で認証されたユーザは、「Admin」（管理者）権限を取得することができます。

パラメータ

パラメータ	説明
default | method_list_name <string15>	• default - ユーザに定義されたアクセス認証のためのデフォルトメソッドリスト。 • method_list_name <string 15> - ユーザによって定義されたメソッドリスト名を入力します。（create authen_enable）
method {tacacs | xtacacs |tacacs+ | radius | server_group <string 15> | local_enable | none}	本メソッドリストに追加する認証方法を最大 4 件まで指定します。 • tacacs - リモートの TACACS サーバから TACACS プロトコルを使用してユーザ認証を行います。 • xtacacs - リモートの XTACACS サーバから XTACACS プロトコルを使用してユーザ認証を行います。 • tacacs+ - リモートの TACACS+ サーバから TACACS+ プロトコルを使用してユーザ認証を行います。 • radius - リモートの RADIUS サーバから RADIUS プロトコルを使用してユーザ認証を行います。 • server_group <string 15> - スイッチに設定したユーザ定義のサーバグループを使用してユーザ認証を行います。 • local - スイッチ上のローカルユーザアカウントデータベースを使用してユーザ認証を行います。 • none - スイッチへアクセスするために認証要求はしません。

使用例

認証メソッド tacacs、xtacacs および local をこの順番でユーザ定義メソッドリスト「DLee」を設定します。

```
DES-3526:admin#config authen_enable method_list_name DLee method tacacs xtacacs
local
Command: config authen_enable method_list_name DLee method tacacs xtacacs local

Success.

DES-3526:admin#
```

認証メソッド tacacs、xtacacs および local をこの順番でデフォルトメソッドリストを設定します。

```
DES-3526:admin#config authen_enable default method xtacacs tacacs+ local
Command: config authen_enable default method xtacacs tacacs+ local

Success.

DES-3526:admin#
```

delete authen_enable method_list_name

目的

ノーマルユーザ権限を管理者権限に昇格するための認証方法を規定するユーザ定義のログインメソッドリストを削除します。

構文

delete authen_enable method_list_name <string 15>

説明

ノーマルユーザ権限を管理者権限に昇格するための認証方法を規定するユーザ定義のログインメソッドリストを削除します。

パラメータ

パラメータ	説明
method_list_name <string 15>	15 文字以内の半角英数字の文字列で、削除するメソッドリスト名を入力します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ユーザ定義のメソッドリスト「Permit」を削除します。

```
DES-3526:admin#delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit

Success.

DES-3526:admin#
```

show authen_enable

目的

ノーマルユーザ権限を管理者権限に昇格するための認証方法を規定するユーザ定義のログインメソッドリストを表示します。

構文

show authen_enable [default | method_list_name <string 15> | all]

説明

ノーマルユーザ権限を管理者権限に昇格するための認証方法を規定するユーザ定義のログインメソッドリストを表示します。

パラメータ

スイッチの管理者レベルにアクセスを昇格するように試みるユーザのデフォルトメソッドリストを表示します。

パラメータ	説明
default	デフォルトのメソッドリストを表示します。
method_list_name <string 15>	15 文字以内の半角英数字の文字列で、参照するメソッドリスト名を入力します。
all	現在スイッチに設定されているすべての認証ログインメソッドを表示します。

画面には以下のパラメータが表示されます。

パラメータ	説明
Method List Name	設定されているメソッドリスト名。
Priority	ユーザがスイッチにログインする場合、認証のために問い合わせされるメソッドリストプロトコルの順番を定義します。優先順位は 1（最も高い）から 4（最も低い）です。
Method Name	メソッドリスト名ごとに実行されるセキュリティプロトコルを定義します。
Comment	メソッドのタイプを定義します。ユーザ定義のグループは、ユーザが定義したサーバグループを参照します。実装されているグループは、スイッチ内の普遍設定である tacacs、xtacacs、tacacs+ および radius セキュリティプロトコルを参照します。キーワードは local（スイッチのユーザアカウント経由の認証）と none（スイッチのすべての機能にアクセスするために認証は必要なし）という tacacs/xtacacs/tacacs+/radius の代わりの技術を使用して認証を参照します。

制限事項

なし。

使用例

ユーザ権限を管理者権限に昇格するためのすべてのメソッドリストを表示します。

```
DES-3526:admin#show authen_enable all
Command: show authen_enable all

Method List Name Priority    Method Name Comment
---------------- ----------- ----------- -------------------
Permit           1             tacacs+   Built-in Group
                 2             tacacs    Built-in Group
                 3             ctsnow    User-defined Group
                 4             local     Keyword

default          1             tacacs+   Built-in Group
                 2             local     Keyword

Total Entries :2

DES-3526:admin#
```

config authen application

目的

設定済みのメソッドリストを使用して、認証のためにスイッチに様々なアプリケーションを設定します。

構文

config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]

説明

作成済みのメソッドリストを使用して、ユーザレベルおよび管理者レベル（authen_enable）でログインする際に使用するスイッチの設定用アプリケーション（コンソール、Telnet、SSH、Web）を設定します。

パラメータ

パラメータ	説明
application [console | telnet | ssh | http | all]	設定するアプリケーションを選択します。以下の 5 つのオプションから 1 つを選択します。 • console - コマンドラインインタフェースログインメソッドを設定します。 • telnet - telnet ログインメソッドを設定します。 • ssh - Secure Shell ログインメソッドを設定します。 • http - Web インタフェースログインメソッドを設定します。 • all - すべてのアプリケーション（コンソール、Telnet、SSH、Web）ログインメソッドを設定します。
login | enable	• login - 登録済みのメソッドリストを使用して、ユーザレベルの通常ログインを行うアプリケーションを設定します。 • enable - 登録済みのメソッドリストを使用して、通常のユーザレベルを管理者権限に昇格させるアプリケーションを設定します。
default | method_list_name <string 15>	• default - デフォルトメソッドリストを使用して、ユーザ認証を行うアプリケーションを設定します。 • method_list_name <string 15> - 登録済みのメソッドリストを使用して、ユーザ認証用のアプリケーションを設定します。15 文字以内の半角英数字の文字列を入力して、登録済みのメソッドリストを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

Web インタフェースのためにデフォルトメソッドリストを設定します。

```
DES-3526:admin#config authen application http login default
Command: config authen application http login default

Success.

DES-3526:admin#
```

show authen application

目的

スイッチの様々なアプリケーションのための認証方法を表示します。

構文

show authen application

説明

スイッチに現在設定されているスイッチ設定アプリケーション（コンソール、Telnet、SSH、Web）に対するすべての認証メソッドリスト（ログイン、管理者特権の有効化など）を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチのすべてのアプリケーションに対するログインと enable method list を表示します。

```
DES-3526:admin#show authen application
Command: show authen application

Application Login Method List Enable Method List
----------- ----------------- ------------------
Console     default           default
Telnet      DLee              default
SSH         default           default
HTTP        default           default

DES-3526:admin#
```

create authen server_group

目的

ユーザ定義の認証サーバグループを作成します。

構文

create authen server_group <string 15>

説明

認証サーバグループを作成します。サーバグループとは、TACACS/XTACACS/TACACS+/RADIUS のサーバホストを、ユーザ定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。本コマンドを使用して、8 個の認証サーバホストをこのグループに追加することができます。

パラメータ

パラメータ	説明
server_group <string 15>	15 文字以内の半角英数字の文字列を入力して、enable メソッドリストを作成します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

サーバグループ「group_1」を作成します。

```
DES-3526:admin#create authen server_group group_1
Command: create authen server_group group_1

Success.

DES-3526:admin#
```

config authen server_group

目的

ユーザ定義の認証サーバグループを設定します。

構文

config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

説明

認証サーバグループを設定します。サーバグループとは、TACACS/XTACACS/TACACS+/RADIUS のサーバホストを、ユーザ定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。プロトコルによって、または定義済みのサーバグループに組み込むことによりグループ分けを行います。どのグループにも最大 8 個までの認証サーバホストを登録できます。

パラメータ

パラメータ	説明
server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>]	スイッチに実装するプロトコルグループ（TACACS/XTACACS/TACACS+/RADIUS）、または「create authen server_group」コマンドで作成したユーザ定義グループによってグループを定義します。 • tacacs - スイッチに実装されている TACACS サーバプロトコルを使用します。TACACS プロトコルを使用するサーバホストだけをこのグループに追加することができます。 • xtacacs - スイッチに実装されている XTACACS サーバプロトコルを使用します。XTACACS プロトコルを使用するサーバホストだけをこのグループに追加することができます。 • tacacs+ - スイッチに実装されている TACACS+ サーバプロトコルを使用します。TACACS+ プロトコルを使用するサーバホストだけをこのグループに追加することができます • radius - スイッチに実装されている RADIUS サーバプロトコルを使用します。RADIUS プロトコルを使用するサーバホストだけをこのグループに追加することができます • <string 15> - 15 文字以内の半角英数字の文字列を入力して、作成済みのサーバグループを指定します。本グループはプロトコルにかかわらずサーバホストのどんな組み合わせも追加することができます。
add | delete	サーバグループからサーバホストを追加または削除します。
server_host<ipaddr>	追加または削除するリモートサーバホストの IP アドレスを入力します。
protocol [tacacs | xtacacs | tacacs+ | radius]	サーバホストが使用するプロトコルを入力します。以下のオプションがあります。 • tacacs - サーバホストが TACACS 認証プロトコルを使用している場合に指定します。 • xtacacs - サーバホストが XTACACS 認証プロトコルを使用している場合に指定します。 • tacacs+ - サーバホストが TACACS+ 認証プロトコルを使用している場合に指定します。 • radius - サーバホストが RADIUS 認証プロトコルを使用している場合に指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

サーバグループ「group_1」に認証ホストを追加します。

```
DES-3526:admin#config authen server_group group_1 add server_host 10.1.1.121 protocol
tacacs+
Command: config authen server_group group_1 add server_host 10.1.1.121 protocol tacacs+

Success.

DES-3526:admin#
```

delete authen server_group

目的

ユーザ定義の認証サーバホストグループを削除します。

構文

delete authen server_group <string 15>

説明

認証サーバグループを削除します。

パラメータ

パラメータ	説明
server_group <string 15>	15 文字以内の半角英数字の文字列を入力して、削除するメソッドリストを指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

サーバグループ「group_1」を削除します。

```
DES-3526:admin#delete server_group group_1
Command: delete server_group group_1

Success.

DES-3526:admin#
```

show authen server_group

目的

スイッチの認証サーバグループを表示します。

構文

show authen server_group {<string 15>}

説明

スイッチに設定されている現在の認証サーバグループを表示します。

パラメータ

パラメータ	説明
server_group <string 15>	15 文字以内の半角英数字の文字列を入力して、参照するサーバグループを指定します。 本コマンドを <string> パラメータなしで入力すると、スイッチのすべての認証サーバグループを表示します。
Group Name	実装されているグループおよびユーザ定義グループを含むスイッチに現在設定されているサーバグループの名前。
IP Address	認証サーバホストの IP アドレス。
Protocol	サーバホストが使用するプロトコル。

制限事項

なし。

使用例

スイッチに現在設定している認証サーバホストを参照します。

```
DES-3526:admin#show authen server_group
Command: show authen server_group

Group Name IP Address  Protocol
---------- ----------- --------
Darren     10.53.13.2  TACACS
tacacs     10.53.13.94 TACACS
tacacs+    (This group has no entry)
xtacacs    (This group has no entry)

Total Entries :4

DES-3526:admin#
```

create authen server_host

目的

認証サーバホストを作成します。

構文

create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}

説明

本コマンドでは、スイッチに TACACS/ XTACACS/ TACACS+/ RADIUS セキュリティプロトコルに対応したユーザ定義の認証サーバホストを作成します。ユーザが認証ポリシーを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/ XTACACS/ TACACS+/ RADIUS サーバホストに認証パケットを送信します。すると TACACS/ XTACACS/ TACACS+/ RADIUS サーバホストはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/ XTACACS/ TACACS+/ RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。サポート可能なサーバホストは最大 16 台です。

パラメータ

パラメータ	説明
server_host <ipaddr>	追加するリモートサーバホストの IP アドレス。
protocol [tacacs | xtacacs | tacacs+ | radius]	サーバホストが使用するプロトコル。以下から選択します。 • tacacs - サーバホストが TACACS プロトコルを使用している場合に選択します。 • xtacacs - サーバホストが XTACACS プロトコルを使用している場合に選択します。 • tacacs+ - サーバホストが TACACS+ プロトコルを使用している場合に選択します。 • radius - サーバホストが RADIUS プロトコルを使用している場合に選択します
port <int 1-65535>	サーバホスト上で認証プロトコルに使用する仮想ポート番号（1-65535）。ポート番号の初期値は、TACACS/ XTACACS/TACACS+ サーバの場合は 49、RADIUS サーバの場合は 1812 および 1813 です。独自の番号を設定してセキュリティを向上することも可能です。
key [<key_string 254> | none]	TACACS+ と RADIUS サーバの場合に指定する共有キー。254 文字までの半角英数字または「none」を指定します。
timeout <int 1-255>	スイッチが、サーバホストからの認証リクエストへの応答を待つ時間（秒）。初期値は 5（秒）です。
retransmit <int 1-255>	サーバからの応答がない場合に、デバイスが認証リクエストを再送する回数。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート番号が 1234、タイムアウトの値が 10 秒、再送回数が 5 である TACACS+ 認証サーバホストを作成します。

```
DES-3526:admin#create authen server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10
retransmit 5
Command: create authen server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10 retransmit 5

Success.

DES-3526:admin#
```

config authen server_host

目的

ユーザ定義の認証サーバホストを設定します。

構文

config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <1-255>}

説明

スイッチに TACACS/XTACACS/TACACS+/RADIUS セキュリティプロトコルに対応したユーザ定義の認証サーバホストを設定します。ユーザが認証プロトコルを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/XTACACS/TACACS+/RADIUS サーバホストに認証パケットを送信します。すると TACACS/XTACACS/TACACS+/RADIUS サーバホストはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/XTACACS/TACACS+/RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。サポート可能なサーバホストは最大 16 台です。

パラメータ

パラメータ	説明
server_host <ipaddr>	変更するリモートサーバホストの IP アドレス。
protocol [tacacs | xtacacs | tacacs+ | radius]	サーバホストが使用するプロトコル。以下から選択します。 • tacacs - サーバホストが TACACS プロトコルを使用している場合に選択します。 • xtacacs - サーバホストが XTACACS プロトコルを使用している場合に選択します。 • tacacs+ - サーバホストが TACACS+ プロトコルを使用している場合に選択します。 • radius - サーバホストが RADIUS プロトコルを使用している場合に選択します
port <int 1-65535>	サーバホスト上で認証プロトコルに使用する仮想ポート番号（1-65535）。ポート番号の初期値は、TACACS/XTACACS/TACACS+ サーバの場合は 49、RADIUS サーバの場合は 1812 および 1813 です。独自の番号を設定してセキュリティを向上することも可能です。
key [<key_string 254> | none]	TACACS+ と RADIUS サーバの場合に指定する共有キー。254 文字までの半角英数字または「none」を指定します。
timeout <int 1-255>	スイッチが、サーバホストからの認証リクエストへの応答を待つ時間（秒）。初期値は 5（秒）です。
retransmit <int 1-255>	サーバからの応答がない場合に、デバイスが認証リクエストを再送する回数。本フィールドでは TACACS+ プロトコルは操作できません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ポート番号が 4321、タイムアウトの値が 12 秒、TACACS+ 認証サーバホストを作成します。

```
DES-3526:admin#config authen server_host 10.1.1.121 protocol tacacs+ port 4321 timeout
12
Command: config authen server_host 10.1.1.121 protocol tacacs+ port 4321 timeout 12

Success.

DES-3526:admin#
```

delete authen server_host

目的

ユーザ定義の認証サーバホストを削除します。

構文

delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

説明

登録済みのユーザ定義認証サーバホストを削除します。

パラメータ

パラメータ	説明
server_host <ipaddr>	削除するリモートサーバホストの IP アドレス。
protocol [tacacs | xtacacs | tacacs+ | radius]	削除するサーバホストが使用するプロトコル。以下から選択します。 • tacacs - サーバホストが TACACS プロトコルを使用している場合に選択します。 • xtacacs - サーバホストが XTACACS プロトコルを使用している場合に選択します。 • tacacs+ - サーバホストが TACACS+ プロトコルを使用している場合に選択します。 • radius - サーバホストが RADIUS プロトコルを使用している場合に選択します

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ユーザ定義の TACACS+ 認証サーバホストを削除します。

```
DES-3526:admin#delete authen server_host 10.1.1.121 protocol tacacs+
Command: delete authen server_host 10.1.1.121 protocol tacacs+

Success.

DES-3526:admin#
```

show authen server_host

目的

ユーザ定義の認証サーバホストを参照します。

構文

show authen server_host

説明

登録済みのユーザ定義認証サーバホストを参照します。

パラメータ

パラメータ	説明
IP Address	認証サーバホストの IP アドレス。
protocol	サーバホストが使用するプロトコル。結果には TACACS、XTACACS、TACACS+ または RADIUS が含まれる可能性が高くなります。
Port	サーバホストの仮想ポート番号。初期値は 49 です。
Timeout	スイッチが、サーバホストからの認証リクエストへの応答を待つ時間（秒）。
Retransmit	TACACS サーバからの応答がない場合に、デバイスが認証リクエストを再送する回数。本フィールドでは TACACS+ プロトコルは操作できません。
Key	設定済みの TACACS+ サーバと共有する認証キー。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに現在設定している認証サーバホストを参照します。

```
DES-3526:admin#show authen server_host
Command: show authen server_host

IP Address  Protocol Port Timeout Retransmit Key
----------- -------- ---- ------- ---------- ------
10.53.13.94 TACACS   49    5      2          No Use

Total Entries :1

DES-3526:admin#
```

config authen parameter response_timeout

目的

スイッチが、タイムアウトの前にユーザからの認証のレスポンスを待つ時間を設定します。

構文

config authen parameter response_timeout <int 0-255>

説明

ユーザからの認証のレスポンスに対するスイッチの待ち時間を指定します。

パラメータ

パラメータ	説明
response_timeout <int 0-255>	コマンドラインインタフェースまたは telnet インタフェースからユーザの認証レスポンスに対するスイッチの待ち時間を指定します。0-255（秒）の範囲から指定します。0 はタイムアウトにならないことを意味します。初期値は 30（秒）です。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

60 秒のレスポンスのタイムアウトを設定します。

```
DES-3526:admin#config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DES-3526:admin#
```

config authen parameter attempt

目的

ユーザが認証を試みることができる最大回数を設定します。

構文

config authen parameter attempt <int 1-255>

説明

ユーザが認証を試みることができる最大回数。指定回数認証に失敗すると、そのユーザはスイッチへのアクセスを拒否され、さらに認証を試みることができなくなります。CLI ユーザは、再度認証を行うために 60 秒待つ必要があります。Telnet ユーザはスイッチから切断されます。

パラメータ

パラメータ	説明
parameter attempt <int 1-255>	ユーザがスイッチによる認証のために試みることができる最大回数を設定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

許可される認証試みの最大数に 5 を設定します。

```
DES-3526:admin#config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

DES-3526:admin#
```

show authen parameter

目的

スイッチに現在設定されている認証パラメータを表示します。

構文

show authen parameter

説明

レスポンスタイムアウトおよびユーザ認証を試みる回数を含むスイッチに設定されている現在の認証パラメータを表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに現在設定している認証パラメータを参照します。

```
DES-3526:admin#show authen parameter
Command: show authen parameter

Response timeout :60 seconds
User attempts    :5

DES-3526:admin#
```

enable admin

目的

ユーザレベルから管理者レベルに権限を昇格します。

構文

enable admin

説明

通常のユーザレベルとしてスイッチにログインした後、管理者レベルに変更する場合に使用します。スイッチにログインした後のユーザにはユーザレベルの権限のみが与えられています。管理者レベルの権限を取得するためには、本コマンドを入力し、認証用パスワードを入力します。本機能における認証方法には、TACACS/XTACACS/TACACS+/RADIUS、ユーザ定義のサーバグループ、local enable（スイッチのローカルアカウント）または、認証なし（none）があります。XTACACS と TACACS は Enable の機能をサポートしていないため、ユーザはサーバホストに特別なアカウントを作成し、ユーザ名「enable」、および管理者が設定するパスワードを登録する必要があります。本機能は認証ポリシーが「disable」（無効）である場合には実行できません。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチで管理者レベルの権限を有効にします。

```
DES-3526:admin#enable admin
Command: enable admin
Password:******

DES-3526:admin#
```

config admin local_enable

目的

本コマンドは、通常のユーザレベルとしてスイッチにログインした後、管理者レベルに変更したい場合に使用します。スイッチにログインした後のユーザにはユーザレベルの権限のみが与えられています。管理者レベルの権限を取得するためには、本画面を開き、認証用パスワードを入力します。本機能における認証方法は、TACACS/ XTACACS/ TACACS+/ RADIUS、ユーザ定義のサーバグループ、local enable（スイッチ上のローカルアカウント）または、認証なし（none）から選択できます。XTACACS と TACACS は Enable の機能をサポートしていないため、ユーザはサーバホスト上に特別なアカウントを作成し、ユーザ名「enable」、および管理者が設定するパスワードを登録する必要があります。本機能は認証ポリシーが「disable」（無効）である場合には実行できません。

構文

config admin local_enable

説明

「enable admin」コマンド用の Local Enable Password を設定します。ユーザがその権限をユーザレベルから管理者レベルに変更する際の認証方法に、「local_enable」を選択している場合、スイッチにローカルに登録したパスワードの入力が要求されます。

パラメータ

パラメータ	説明
<password 15>	本コマンドを入力した後、ユーザは元のパスワード、次に新しいパスワード、さらに確認のために再び新しいパスワードを入力します。パスワードは 15 文字以内の半角英数字で指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

「local_enable」認証方法のためのパスワードを設定します。

```
DES-3526:admin#config admin local_enable
Command: config admin local_enable

Enter the old password:
Enter the case-sensitive new password:******
Enter the new password again for confirmation:******
Success.

DES-3526:admin#
```

第 33 章　SSH コマンド

リモート PC（SSH クライアント）とスイッチ（SSH サーバ）間でセキュアな通信を行うための SSH プロトコルの設定は、以下の手順で行います。

1. 「create account admin」コマンドで管理者レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに管理者レベルのユーザアカウントを作成する方法と同じで、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。

2. 「config ssh user」コマンドを使用して、ユーザアカウントを設定します。この時スイッチが SSH 接続の確立を許可する際のユーザの認証方法を指定します。この認証方法には、「password」、「publickey」、「hostbased」の 3 つがあります。

3. SSH クライアントとサーバ間で送受信するメッセージの暗号化、復号化に用いる暗号化アルゴリズムを設定します。

4. 最後に「enable ssh」コマンドで、SSH を有効にします。

これらの手順が完了後、安全な帯域内の通信を使用してリモート PC 上の SSH クライアントの設定とスイッチの管理を行うことができます。

コマンドラインインタフェース（CLI）における Secure Shell（SSH）コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable ssh	
disable ssh	
config ssh authmode	[password | publickey | hostbased] [enable | disable]
show ssh authmode	
config ssh server	{maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never]
show ssh server	
config ssh user	<username> authmode [hostbased [hostname <domain_name> | hostname_IP <domain_name> <ipaddr>] | password | publickey]
show ssh user authmode	
config ssh algorithm	[3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm	
config ssh regenerate hostkey	

以下のセクションで各コマンドについて詳しく説明します。

enable ssh

目的

SSH を有効にします。

構文

enable ssh

説明

スイッチの SSH を有効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。SSH を有効にすると、スイッチの Telnet マネージャは無効になります。

使用例

SSH を有効にします。

```
DES-3526:admin#enable ssh
Command: enable ssh

Success.

DES-3526:admin#
```

disable ssh

目的

SSH を無効にします。

構文

disable ssh

内容

スイッチの SSH を無効にします。

パラメータ

なし。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。SSH を有効にすると、スイッチの Telnet マネージャは無効になります。

使用例

SSH を無効にします。

```
DES-3526:admin#disable ssh
Command: disable ssh

Success.

DES-3526:admin#
```

config ssh authmode

目的

スイッチの SSH 認証設定を行います。

構文

config ssh authmode [password | publickey | hostbased] [enable | disable]

説明

スイッチにアクセスを試みるユーザのために SSH 認証モードを設定します。

パラメータ

パラメータ	説明
password | publickey | hostbased	• password - スイッチにおける認証にローカルに設定したパスワードを使用します。 • publickey - スイッチにおける認証に SSH サーバに設定した公開鍵を使用します。 • hostbased - 認証にホストコンピュータを使用します。本パラメータは SSH 認証機能を必要とする Linux ユーザ向けに設定されます。ホストコンピュータには SSH プログラムがインストールされ、Linux OS が起動している必要があります。
[enable | disable]	指定された SSH 認証を有効または無効にします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

パスワードによる SSH 認証モードを有効にします。

```
DES-3526:admin#config ssh authmode password enable
Command: config ssh authmode password enable

Success.

DES-3526:admin#
```

show ssh authmode

目的

SSH 認証モード設定を表示します。

構文

show ssh authmode

説明

スイッチの現在の SSH 認証設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチの現在の認証モード設定を表示します。

```
DES-3526:admin#show ssh authmode
Command: show ssh authmode

The SSH authmode:
---------------------
Password  :Enabled
Publickey :Enabled
Hostbased :Enabled

DES-3526:admin#
```

config ssh server

目的

SSH サーバを設定します。

構文

config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never]}

説明

スイッチに SSH サーバ設定のパラメータを設定します。

パラメータ

パラメータ	説明
maxsession <int 1-8>	同時にスイッチに接続できる数を 1 から 8 の数字を設定します。初期値は 8 です。
contimeout <sec 120-600>	接続のタイムアウト時間を指定します。120 から 600（秒）を設定します。初期値は 300（秒）です。
authfail <int 2-20>	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。指定した回数を超えるとスイッチは接続を切り、ユーザは再度スイッチに接続する必要があります。
rekey [10min | 30min | 60min | never]	スイッチが SSH 暗号を変更する期間を設定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

SSH サーバを設定します。

```
DES-3526:admin#config ssh server maxsession 2 contimeout 300 authfail 2
Command: config ssh server maxsession 2 contimeout 300 authfail 2

Success.

DES-3526:admin#
```

show ssh server

目的

SSH 認証サーバ設定を表示します。

構文

show ssh server

説明

スイッチの現在の SSH サーバ設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

SSH サーバを表示します。

```
DES-3526:admin#show ssh server
Command: show ssh server

SSH Server Status             :Disabled
SSH Max Session               :8
Connection timeout            :300(sec)
Authenticate failed attempts :2
Rekey timeout                 :never
Listened Port Number          :22

DES-3526:admin#
```

config ssh user

目的

SSH ユーザを設定します。

構文

config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr>] | password | publickey]

説明

スイッチに SSH ユーザ認証方式を設定します。

パラメータ

パラメータ	説明
<username 15>	SSH ユーザを識別するユーザ名を 15 文字までの半角英数字で指定します。
authmode	スイッチへのログインを希望する SSH ユーザの認証モードを指定します。管理者は以下のパラメータを選択することができます。
hostbased	認証用にリモート SSH サーバを使用する場合に選択します。本パラメータを選択すると、SSH ユーザ識別のために「Host Name」および「Host IP」フィールドの入力が必要になります。
hostname <domain_name 32>	リモートの SSH ユーザを識別する 32 文字以内の半角英数字の文字列を入力します。
hostname_IP <domain_name 32> <ipaddr>	SSH ユーザのホスト名と対応する IP アドレスを入力します。
password	管理者定義のパスワードを使用してユーザ認証を行う場合に選択します。本パラメータを選択すると、スイッチは管理者にパスワードの入力（確認のため 2 回）を促します。
publickey	SSH サーバ上の公開鍵を使用して認証を行う場合に選択します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

SSH ユーザを設定します。

```
DES-3526:admin#config ssh user Trinity authmode Password
Command: config ssh user Trinity authmode Password

Success.

DES-3526:admin#
```

show ssh user authmode

目的

SSH 認証ユーザ設定を表示します。

構文

show ssh user authmode

説明

スイッチの現在の SSH ユーザ設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチの現在の SSH ユーザ設定を表示します。

```
DES-3526:admin#show ssh user authmode
Command: show ssh user authmode

Current Accounts:
Username  AuthMode   HostName  HostIP
--------  ---------  --------  ----------
Trinity   Hostbased  Zira      10.45.25.8

Total Entries = 1

DES-3526:admin#
```

注意 SSH ユーザを設定するためには、管理者はスイッチにユーザアカウントを作成する必要があります。ユーザアカウント設定に関する情報については、本マニュアル「第 4 章 基本のスイッチコマンド」の「create account user」コマンドを参照してください。

config ssh algorithm

目的

SSH アルゴリズムを設定します。

構文

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]

説明

認証の暗号化に使用する SSH アルゴリズムの種類を設定します。

パラメータ

パラメータ	説明
3DES	Triple_Data EtiStddtilithEncryption Standard 暗号化アルゴリズムを有効または無効にします。
AES128	AES 128 暗号化アルゴリズムを有効または無効にします。
AES192	AES 192 暗号化アルゴリズムを有効または無効にします。
AES256	AES 256 暗号化アルゴリズムを有効または無効にします。
arcfour	arcfour 暗号化アルゴリズムを有効または無効にします。
blowfish	Blowfish 暗号化アルゴリズムを有効または無効にします。
cast128	Cast128 暗号化アルゴリズムを有効または無効にします。
twofish128	Twofish 128 暗号化アルゴリズムを有効または無効にします。
twofish192	Twofish 192 暗号化アルゴリズムを有効または無効にします。
twofish256	Twofish 256 暗号化アルゴリズムを有効または無効にします。
MD5	MD5 暗号化アルゴリズムを有効または無効にします。
SHA1	Secure Hash Algorithm 暗号化を有効または無効にします。
RSA	RSA 暗号化アルゴリズムを有効または無効にします。
DSA	Digital Signature Algorithm 暗号化を有効または無効にします。
[enable | disable]	本コマンドで入力したアルゴリズムを有効または無効にします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

SSH アルゴリズムを設定します。

```
DES-3526:admin#config ssh algorithm Blowfish enable
Command: config ssh algorithm Blowfish enable

Success.

DES-3526:admin#
```

show ssh algorithm

目的

SSH アルゴリズム設定を表示します。

構文

show ssh algorithm

説明

現在の SSH アルゴリズム設定状態を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチに現在設定されている SSH アルゴリズムを表示します。

```
DES-3526:admin#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
----------------------
3DES       :Enabled
AES192     :Enabled
AES256     :Enabled
arcfour    :Enabled
cast128    :Enabled
twofish128 :Enabled
twofish192 :Enabled
twofish256 :Enabled

Data Integrity Algorithm
------------------------
MD5  :Enabled
SHA1 :Enabled

Public Key Algorithm
------------------------
RSA :Enabled
DSA :Enabled

DES-3526:admin#
```

config ssh regenerate hostkey

目的

SSH アルゴリズム設定のためのホストキーを再生します。

構文

config ssh regenerate hostkey

説明

SSH アルゴリズム設定のためのホストキーを再生します。

パラメータ

なし。

制限事項

なし。

使用例

SSH アルゴリズム設定のためのホストキーを再生します。

```
DES-3526:admin#? config ssh regenerate hostkey
Command: ? config ssh regenerate hostkey

Command: config ssh regenerate hostkey
Usage:

DES-3526:admin#
```

第 34 章　SSL コマンド

Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。このセキュリティ機能は、認証セッションに使用する厳密な暗号パラメータ、特定の暗号化アルゴリズムおよびキー長を決定する、暗号スイートと呼ばれるセキュリティ文字列により実現しています。SSL は、以下の 3 つの段階で構成されます。

1. 鍵交換
   暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。本レベルは、鍵を交換して適合する相手を探し、暗号化のネゴシエーションを行うまでの認証を行って、次のレベルに進むというクライアント、ホスト間の最初のプロセスとなります。
2. 暗号化
   暗号スイートの次の段階は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
   - ストリーム暗号 – スイッチは 2 種類のストリーム暗号に対応します。1 つは 40 ビット鍵での RC4、もう 1 つは 128 ビット鍵での RC4 です。これらの鍵はメッセージの暗号化に使用され、最適な使用のためにはクライアントとホスト間で一致させる必要があります。
   - CBC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、前に暗号化したブロックの暗号文を使用して現在のブロックの暗号化を行う方法です。本スイッチは、DES（Data Encryption Standard）で定義する 3 DES EDE 暗号化コードをサポートし、暗号文を生成します。
3. ハッシュアルゴリズム
   暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージで暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5（Message Digest 5）と SHA（Secure Hash Algorithm）の 2 種類のハッシュアルゴリズムをサポートします。

これら 3 つのパラメータは、スイッチ上での 4 つの選択肢として独自に組み合わされ、サーバとホスト間で安全な通信を行うための 3 層の暗号化コードを生成します。暗号スイートの中から 1 つ、または複数を組み合わせて実行することができますが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれるファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバを使用してスイッチにダウンロードできます。本スイッチは、SSLv3 をサポートしています。SSL の他のバージョンは本スイッチとは互換性がないおそれがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する場合があります。

コマンドラインインタフェース（CLI）における Secure Sockets Layer（SSL）コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
disable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
config ssl cachetimeout	<value 60-86400>
show ssl cachetimeout	
show ssl	
download certificate_fromTFTP	<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>

次のセクションで各コマンドについて詳しく説明します。

enable ssl

目的

スイッチの SSL 機能を有効にします。

構文

enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}

説明

ネットワークマネージャが SSL を有効にしてスイッチに暗号スイートを設定できます。本コマンドをパラメータなしで入力すると、スイッチの SSL 状態は無効になります。SSL 機能が有効になると Web ベースマネジメントは無効になります。

パラメータ

パラメータ	説明
ciphersuite	暗号スイートは認証セッションに使用する、正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定する文字列です。ユーザは以下のどの組み合わせも選択できます。 • RSA_with_RC4_128_MD5 - この暗号スイートは RSA key exchange、stream cipher C4（128-bit keys）、MD5 Hash Algorithm の組み合わせです。 • RSA_with_3DES_EDE_CBC_SHA - この暗号スイートは RSA key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。 • DHE_DSS_with_3DES_EDE_CBC_SHA - この暗号スイートは DSA Diffie Hellman key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。 • RSA_EXPORT_with_RC4_40_MD5 - この暗号スイートは RSA Export key exchange、stream cipher RC4（40-bit keys）、MD5 Hash Algorithm の組み合わせです。 スイッチは SSL 機能のための 4 つの暗号スイートを持ち、初期設定ではすべてを有効にしていますが、暗号スイートを持つ SSL を有効にして、他の SSL を無効にすることも可能です。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

すべての暗号スイートの SSL を有効にします。

```
DES-3526:admin#enable ssl
Command: enable ssl

Note:Web will be disabled if SSL is enabled.
Success.

DES-3526:admin#
```

注意 スイッチの SSL を有効にすると、すべての暗号スイートとなります。特定の暗号スイートを使用するためには、適切な暗号スイートとともに「disable ssl」コマンドで他の暗号スイートを無効にする必要があります。

注意 スイッチの SSL を有効にすると、スイッチは Web マネージャ用のポート（ポート 80）を無効にします。Web マネージャにログインするためには、URL のエントリは「https://」で始まる必要があります。（例 : https://10.90.90.90）

disable ssl

目的

スイッチの SSL 機能を無効にします。

構文

disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}

説明

スイッチの SSL を無効にし、さらに暗号スイートのどんな組み合わせも無効にすることができます。

パラメータ

パラメータ	説明
ciphersuite	暗号スイートは認証セッションに使用する、正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定する文字列です。ユーザは以下のどの組み合わせも選択できます。 • RSA_with_RC4_128_MD5 - この暗号スイートは RSA key exchange、stream cipher C4（128-bit keys）、MD5 Hash Algorithm の組み合わせです。 • RSA_with_3DES_EDE_CBC_SHA - この暗号スイートは RSA key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。 • DHE_DSS_with_3DES_EDE_CBC_SHA - この暗号スイートは DSA Diffie Hellman key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。 • RSA_EXPORT_with_RC4_40_MD5 - この暗号スイートは RSA Export key exchange、stream cipher RC4（40-bit keys）、MD5 Hash Algorithm の組み合わせです。 スイッチは SSL 機能のための 4 つの暗号スイートを持ち、初期設定ではすべてを有効にしていますが、暗号スイートを持つ SSL を有効にして、他の SSL を無効にすることも可能です。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチの SSL 状態を無効にします。

```
DES-3526:admin#disable ssl
Command: disable ssl

Success.

DES-3526:admin#
```

暗号スイート RSA_EXPORT_with_RC4_40_MD5 だけを無効にします。

```
DES-3526:admin#disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
Command: disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5

Success.

DES-3526:admin#
```

config ssl cachetimeout

目的

SSL キャッシュタイムアウトを設定します。

構文

config ssl cachetimeout <value 60-86400>

説明

クライアントとホストの間の SSL による新しい鍵交換の間隔を指定します。クライアントとホストが鍵交換をすると常に新しい SSL セッションが確立します。この値を長くすると SSL セッションによる特定のホストとの再接続には主鍵が再利用されます。そのためネゴシエーション処理は速くなります。

パラメータ

パラメータ	説明
<value 60-86400>	60-86400（秒）でタイムアウト時間を設定します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

SSL キャッシュタイムアウトに 7200（秒）を指定します。

```
DES-3526:admin#config ssl cachetimeout 7200
Command: config ssl cachetimeout 7200

Success.

DES-3526:admin#
```

show ssl cachetimeout

目的

SSL キャッシュタイムアウトを参照します。

構文

show ssl cachetimeout

説明

スイッチで現在実行されている SSL キャッシュタイムアウトを参照します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチで現在実行されている SSL キャッシュタイムアウトを参照します。

```
DES-3526:admin#show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 seconds

DES-3526:admin#
```

show ssl

目的

スイッチの SSL と証明書ファイルの状態を参照します。

構文

show ssl {certificate}

説明

登録済みの SSL 状態を参照します。

パラメータ

パラメータ	説明
certificate	スイッチで現在実行している SSL 証明書ファイル情報を参照します。

制限事項

なし。

使用例

スイッチの SSL 状態を参照します。

```
DES-3526:admin#show ssl
Command: show ssl
 SSL status                           Disabled
 RSA_WITH_RC4_128_MD5          0x0004  Enabled
 RSA_with_3DES_EDE_CBC_SHA     0x000A  Enabled
 DHE_DSS_WITH_3DES_EDE_CBC_SHA 0x0013  Enabled
 RSA_EXPORT_WITH_RC4_40_MD5    0x0003  Enabled

DES-3526:admin#
```

スイッチの証明書ファイル情報を参照します。

```
DES-3526:admin#show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DES-3526:admin#
```

download certificate_fromTFTP

目的

スイッチの SSL 機能のために証明書ファイルをダウンロードします。

構文

download certificate_fromTFTP <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>

説明

SSL を使用するための証明書ファイルを TFTP サーバからダウンロードします。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者の情報や認証のための鍵やデジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバとクライアントが一致した証明書ファイルを持つ必要があります。本スイッチは、拡張子 ".der" を持つ証明書のみをサポートします。

パラメータ

パラメータ	説明
<ipaddr>	TFTP サーバの IP アドレスを指定します。
certfilename <path_filename 64>	ダウンロードする証明書ファイルのパスとファイル名を入力します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

スイッチに証明書ファイルをダウンロードします。

```
DES-3526:admin#download ssl certificate 10.53.13.94 certfilename c:/cert.der keyfilename c:/
pkey.der
Command: download ssl certificate 10.53.13.94 certfilename c:/cert.der keyfilename c:/pkey.der

Certificate Loaded Successfully!

DES-3526:admin#
```

第 35 章　ループバック検知コマンド

ループバック検知機能は、特定ポートに生成されたループを検出します。

コマンドラインインタフェース（CLI）におけるループバック検知コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
config loopdetect	{recover_timer [<value 0> | <value 60-1000000>] | interval <value 1-32767> | mode [port-based | vlan-based]}
config loopdetect ports	[<portlist>| all] state [enable | disable]
enable loopdetect	
disable loopdetect	
show loopdetect	
show loopdetect ports	[all | <portlist>]

以下のセクションで各コマンドについて詳しく説明します。

config loopdetect

目的

スイッチにループバック検知機能を設定します。

構文

config loopdetect {recover_timer [<value 0> | <value 60-1000000>] | interval <value 1-32767> | mode [port-based | vlan-based]}

説明

スイッチにループバック検知機能（LBD）を設定します。

パラメータ

パラメータ	説明
recover_timer [<value 0> | <value 60-1000000>]	ループ状態がなくなったかをチェックする時間を決定するためにオートリカバリ (自動復旧) メカニズムが使用する間隔（秒）。60-1000000 で設定します。 0 は特別な値で、オートリカバリメカニズムの無効を意味します。そのため、手動で無効ポートを回復する必要があります。初期値は 60（秒）です。
interval <value 1-32767>	デバイスがループバックイベントを検出するためにすべての CTP(Configuration Test Protocol) パケットを送信する間隔（秒）。1-32767 で設定します。 初期値は 10（秒）です。
mode [port-based | vlan-based]	ループ検出動作モードを選択します。 • port-based - ポートベースモードでは、ポートはループを検知すると、無効となります。 • vlan-based - VLAN ベースモードでは、ポートは、ループを検知にかかわるポートに到達する VLAN パケットを処理することはできません。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

VLAN ベースモードで「recover_timer」を 0、「interval」を 20 に設定します。

```
DES-3526:admin# config loopdetect recover_timer 0 interval 20 mode vlan-based
Command: config loopdetect recover_timer 0 interval 20 mode vlan-based

Success.

DES-3526:admin#
```

config loopdetect ports

目的

スイッチのポートにループバック検知機能を設定します。

構文

config loopdetect ports [<portlist>| all] state [enable | disable]

説明

スイッチ上のインタフェースにループバック検知機能を設定します。

パラメータ

パラメータ	説明
ports [<portlist> | all]	• <portlist>- 設定するポートまたはポート範囲を指定します。 • all - システムのすべてのポートを設定します。
state [enable|disable]	ポートリストに指定されたポートにループバック検知機能を有効または無効にします。初期値では無効に設定されています。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ループバック検知機能を有効にします。

```
DES-3526:admin# config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

DES-3526:admin#
```

enable loopdetect

目的

ループバック検知機能をグローバルに有効にします。

構文

enable loopdetect

説明

ループバック検知機能をグローバルに有効にします。初期値は有効です。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ループバック検知機能をグローバルに有効にします。

```
DES-3526:admin#show loopdetect
Command: show loopdetect

 Loopdetect Global Settings
 ---------------------------
 Loopdetect Status          : Disabled
 Loopdetect Interval        : 10
 Recover Time               : 60
 Mode                       : Port-Based


DES-3526:admin#
```

disable loopdetect

目的

ループバック検知機能をグローバルに無効にします。

構文

enable loopdetect

説明

ループバック検知機能をグローバルに無効にします。初期値は有効です。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ループバック検知機能をグローバルに無効にします。

```
DES-3526:admin#disable loopdetect
Command: disable loopdetect

Success.

DES-3526:admin#
```

show loopdetect

目的

スイッチの現在のループバック検知機能の設定を表示します。

構文

show loopdetect

説明

スイッチの現在のループバック検知機能の設定を表示します。

パラメータ

なし。

制限事項

なし。

使用例

スイッチの現在のループバック検知機能の設定を表示します。

```
DES-3526:admin#show loopdetect
Command: show loopdetect

LBD Global Settings
-------------------------
LBD Status       :Enabled
LBD Interval     :20
LBD Recover Time :60

DES-3526:admin#
```

show loopdetect ports

目的

スイッチの現在のポート単位のループバック検知設定を表示します。

構文

show loopdetect ports [all | <portlist>]

説明

スイッチの現在のポート単位のループバック検知設定とステータスを表示します。

パラメータ

パラメータ	説明
ports [all | <portlist>]	• all - すべてのポートのループバック検知情報を表示します。 • <portlist> - 表示するポートまたはポート範囲を指定します。

制限事項

なし。

使用例

ポートベースモードのポート 1 から 9 のループバック検知状態を表示します。

```
DES-3526:admin#show loopdetect ports 1-9
Command: show loopdetect ports 1-9

Port Loopdetect State    Loop Status
---- ----------------    -----------------
1    Enabled             Normal
2    Enabled             Normal
3    Enabled             Normal
4    Enabled             Normal
5    Enabled             Loop!
6    Enabled             Normal
7    Enabled             Loop!
8    Enabled             Normal
9    Enabled             Normal

DES-3526:admin#
```

VLAN ベースモードのポート 1 から 9 のループバック検知状態を表示します。

```
DES-3526:admin#show loopdetect ports 1-9
Command: show loopdetect ports 1-9

Port Loopdetect State  Loop VLAN
---- ----------------  -----------------
1    Enabled           None
2    Enabled           None
3    Enabled           None
4    Enabled           None
5    Enabled            2
6    Enabled           None
7    Enabled            2
8    Enabled           None
9    Enabled           None

DES-3526:admin#
```

第 36 章　D-Link シングル IP マネジメントコマンド

D-Link シングル IP マネジメントとは、スタックポートまたはモジュールを使用する代わりにイーサネット経由でスイッチをスタックする方法です。D-Link シングル IP マネジメント（以下 SIM と呼びます）機能を搭載するスイッチには、以下の基本的なルールがあります。

- SIM はスイッチのオプション機能であり、有効 / 無効にできます。また、SIM グループはご使用のネットワーク内でスイッチの操作に影響を与えることはありません。
- SIM には 3 つのクラスのスイッチがあります。Commander Switch（CS）はグループのマスタスイッチ、Member Switch（MS）は CS によって SIM グループのメンバとして認識されるスイッチ、Candidate Switch（CaS）は SIM グループに物理的にリンクはしているが、SIM グループのメンバとして認識されていないスイッチです。
- 1 つの SIM グループには、Commander Switch（CS）を 1 つだけ持つことができます。
- 特定の SIM グループ内のすべてのスイッチは、同じ IP サブネット（ブロードキャストドメイン）内にある必要があります。ルータを越えた位置にあるメンバの設定はできません。
- 1 つの SIM グループには、Commander Switch（番号 :0）を含み、最大 33 台のスイッチ（番号 :0-32）が所属できます。
- 同じ IP サブネット（ブロードキャストドメイン）内の SIM グループ数に制限はありませんが、各スイッチは、1 つの SIM グループにしか所属することができません。
- マルチプル VLAN が設定されていると、SIM グループはスイッチ上のマネジメント VLAN だけを使用します。
- SIM は SIM をサポートしていないデバイスを経由することができます。そのため CS から 1 ホップ以上はなれたスイッチを管理することができます。

SIM グループは 1 つのエンティティとして管理されるスイッチのグループです。SIM スイッチは 3 つの異なる役割を持っています。

1. Commander Switch（CS）- グループの管理用デバイスとして手動で設定されるスイッチで、以下の特長を持っています。
   - IP アドレスを 1 つ持つ。
   - 他のシングル IP グループの CS や MS ではない。
   - マネジメント VLAN 経由で MS に接続する。

2. Member Switch（MS）- シングル IP グループに所属するスイッチで、CS からアクセスが可能です。MS は以下の特長を持ちます。
   - 他のシングル IP グループの CS や MS ではない。
   - CS マネジメント VLAN 経由で CS に接続する。

3. Candidate Switch（CaS）-SIM グループに参加する準備が整っているが、まだ MS ではないスイッチです。CaS を SIM グループ内の MS として、本スイッチの機能を使用して手動で登録することが可能です。CaS として登録されたスイッチは、SIM グループには所属せず、以下の特長を持っています。
   - 他のシングル IP グループの CS や MS ではない。
   - CS マネジメント VLAN 経由で CS に接続する。

上記の役割には、以下のルールを適用します。

1. 各デバイスは、まず CaS の状態から始まる。

2. CS は、はじめに CaS に、その後 MS となり、SIM グループの MS へと遷移します。つまり CS から MS へ直接遷移することはできない。

3. ユーザは、CS から CaS へ手動で遷移させることができる。

4. 以下のような場合に MS から CaS に遷移します。
   a. CS を介して CaS として設定される時。
   b. CS から MS への Report パケットがタイムアウトになった時。

5. ユーザが手動で CaS から CS に遷移するように設定できます

6. CS を介して CaS は MS に遷移するように設定されます。

SIM グループの CS として運用するスイッチを 1 台登録した後、スイッチを手動によりグループに追加して MS とします。CS はその後 MS へのアクセスのためにインバンドエントリポイントとして動作します。CS の IP アドレスがグループのすべての MS への経路になり、CS の管理パスワードや認証によって、SIM グループのすべての MS へのアクセスを制御します。

SIM 機能を有効にすると、CS 内のアプリケーションはパケットを処理する代わりに、リダイレクト（宛先変更）します。アプリケーションは管理者からのパケットを復号化し、データの一部を変更し、MS へ送信します。処理後、CS は MS から Response パケットを受け取り、これを符号化して管理者に返送します。

CS が MS に遷移すると、自動的に CS が所属する最初の SNMP コミュニティ（リード権 / ライト権、リード権だけを含む）のメンバになります。しかし、自身の IP アドレスを持つ MS は、グループ内の他のスイッチ（CS を含む）が所属していない SNMP コミュニティに加入することができます。

バージョン 1.6 へのアップグレード

SIM 管理機能強化の目的で、本スイッチシリーズは本リリースでバージョン 1.6 にアップグレードされました。本バージョンでは以下の改善点が加わりました。

1. CS は、再起動または Web での異常検出によって、SIM グループから抜けたメンバスイッチを自動的に再検出する機能が搭載しました。この機能は、以前設定された SIM メンバが再起動の後に発行する Discover パケットと Maintain パケットを使用することにより実現されます。一度 MS の MAC アドレスとパスワードが CS のデータベースに記録され、MS が再起動を行うと、CS はこの MS の情報をデータベースに保存し、MS が再検出された場合、これを SIM ツリーに自動的に戻します。これらのスイッチの再検出のために設定を行う必要はありません。一度保存を行った MS の再検出ができないという場合もあります。たとえば、スイッチの電源がオンになっていない場合、他のグループのメンバとなっている場合、または CS スイッチとして設定された場合は再検出処理をすることができません。

2. 本バージョンでは、以下のファームウェア、コンフィグレーションファイル、およびログファイルのアップロードやダウンロードを複数スイッチに対して行う機能が追加されました。

   - ファームウェア - TFTP サーバからの MS に対してのファームウェアダウンロードがサポートされました。
   - コンフィグレーションファイル - TFTP サーバを使用したコンフィグレーションのダウンロード / アップロード（コンフィグレーションの復元やバックアップ用）が可能になりました。
   - ログ - MS のログファイルを TFTP サーバにアップロード可能になりました。

コマンドラインインタフェース（CLI）における SIM コマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
enable sim	
disable sim	
show sim	{[candidates {<candidate_id 1-32>} | members {<member_id 1-32> } | group {commander_mac <macaddr>}] | neighbor]}
reconfig	{member_id <value 1-32> | exit}
config sim_group	[add <candidate_id 1-32> {<password>} | delete <member_id 1-32>]
config sim	[{[commander {group_name <groupname 64> | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>}
download sim_ms	[firmware | configuration] <ipaddr> <path_filename> {members <mslist> | all}
upload sim_ms	[configuration] <ipaddr> <path_filename> <member_id 1-32>

以下のセクションで各コマンドについて詳しく記述します。

enable sim

目的

スイッチのシングル IP マネジメント（SIM）を有効にします。

構文

enable sim

説明

スイッチの SIM 機能をグローバルに有効にします。本機能が有効にしないと、SIM 機能は適切に機能しません。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチで SIM を有効にします。

```
DES-3526:admin#enable sim
Command: enable sim

Success.
```

disable sim

目的

スイッチのシングル IP マネジメント（SIM）を無効にします。

構文

disable sim

説明

スイッチの SIM 機能をグローバルに無効にします。

パラメータ

なし。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

スイッチで SIM を無効にします。

```
DES-3526:admin#disable sim
Command: disable sim

Success.
```

show sim

目的

スイッチの SIM グループに関する現在の情報を表示します。

構文

show sim {[candidates {<candidate_id 1-32>} | members {<member_id 1-32>} | group {commander_mac <macaddr>}] | neighbor]}

説明

以下のようなスイッチの SIM グループに関する現在の情報を表示します。

- SIM バージョン - スイッチの現在の SIM バージョンを表示します。
- ファームウェアバージョン - スイッチに設定されているファームウェアバージョンを表示します。
- デバイス名 - スイッチのユーザ定義デバイス名を表示します。
- MAC アドレス - スイッチの MAC アドレスを表示します。
- Capabilities - スイッチのタイプ（レイヤ 2 : L2 またはレイヤ 3 : L3）を表示します。
- SIM State - 現在のスイッチの SIM 状態が有効または無効であるかを表示します。
- Role State - CS、MS、CaS を含むスイッチの現在の役割を表示します。スタンドアロンスイッチは、いつも CS です。
- Discovery Interval - スイッチがネットワークに Discovery パケットを送信する間隔（秒）を表示します。
- Hold time - 廃棄または使用する前にスイッチが検出結果を保持する時間（秒）を表示します。

パラメータ

パラメータ	説明
<candidate_id 1-32>	SIM グループの CaS に関する情報を表示します。特定の CaS を参照する場合は、CaS ID 番号（1-32）を入力します。
members <member_id 1-32>	SIM グループのメンバに関する情報を表示します。特定のメンバを参照するためには、1-32 までのメンバ ID を入力します。
group {commander_mac <macaddr>}	SIM グループに関する情報を表示します。特定のグループを見るためには、グループの CS の MAC アドレスを入力します。
neighbor	スイッチの Neighbor デバイスを表示します。Neighbor は SIM スイッチに物理的に接続していても SIM グループのメンバではないスイッチとして定義されます。以下の結果が生成されます。 • Port - Neighbor スイッチにアップリンクしている CS の物理ポート番号を表示します。 • MAC Address - Neighbor スイッチの MAC アドレスを表示します。 • Role - Neighbor スイッチの役割（CS、CaS、MS）を表示します。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

詳細な SIM 情報を参照します。

```
DES-3526:admin#show sim
Command: show sim

SIM Version : VER-1.61
Firmware Version : Build 4.01-B19
Device Name :
MAC Address : 00-35-26-11-11-00
Capabilities : L2
Platform : DES-3526 L2 Switch
SIM State : Enabled
Role State : Commander
Discovery Interval : 60 sec
Hold Time : 180 sec

DES-3526:admin#
```

詳細な SIM 情報を参照します。
CaS ID が指定されると、サマリ内の CaS 情報を表示します。

```
DES-3526:admin#show sim candidates
Command: show sim candidates
ID MAC Address Platform / Hold Firmware Device Name
Capability Time Version
--- ----------------- ------------------------ ----- --------- ----------------
1 00-01-02-03-04-00 DES-3526 L2 Switch 40 4.01-B19 The Man
2 00-55-55-00-55-00 DES-3526 L2 Switch 140 4.01-B19 default master
Total Entries: 2
DES-3526:admin#
```

MS ID が指定された場合、サマリ内のメンバ情報を表示します。

```
DES-3526:admin#show sim member
Command: show sim member
ID MAC Address Platform / Hold Firmware Device Name
Capability Time Version
--- ----------------- ----------------------- ---- --------- ----------------
1 00-01-02-03-04-00 DES-3526 L2 Switch 40 4.01-B19 The Man
2 00-55-55-00-55-00 DES-3526 L2 Switch 140 4.01-B19 default master
Total Entries: 2
DES-3526:admin#
```

グループが指定された場合、サマリ内のグループ情報を表示します。

```
DES-3526:admin#show sim group
Command: show sim group
SIM Group Name : default
ID MAC Address Platform / Hold Firmware Device Name
Capability Time Version
--- ----------------- ----------------------- ----- --------- ----------------
*1 00-01-02-03-04-00 DES-3526 L2 Switch 40 4.01-B19 Trinity
2 00-55-55-00-55-00 DES-3526 L2 Switch 140 4.01-B19 default master
SIM Group Name : SIM2
ID MAC Address Platform / Hold Firmware Device Name
Capability Time Version
--- ----------------- ----------------------- ------ --------- ----------------
*1 00-01-02-03-04-00 DES-3526 L2 Switch 40 4.01-B19 Neo
2 00-55-55-00-55-00 DES-3526 L2 Switch 140 4.01-B19 default master
‘ *’ means commander switch.
DES-3526:admin#
```

SIM Neighbor を参照します。

```
DES-3526:admin#show sim neighbor
Command: show sim neighbor
Port MAC Address Role
---- ----------------- ---------
23 00-35-26-00-11-99 Commander
23 00-35-26-00-11-91 Member
24 00-35-26-00-11-90 Candidate
Total Entries:3
DES-3526:admin#
```

reconfig

目的

Telnet を使用して、CS から MS に接続します。

構文

reconfig [member_id <value 1-32> | exit]

説明

Telnet を使用して MS に再接続します。

パラメータ

パラメータ	説明
member_id <value 1-32>	設定する MS の ID 番号を指定します。
exit	MS の管理を終了し、CS の管理に戻ります。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

CLI を使用して、CS からメンバ ID2 を持つ MS に接続します。

```
DES-3526:admin#reconfig member_id 2
Command: reconfig member_id 2

DES-3526:admin#
Login:
```

config sim_group

目的

SIM グループから CaS の追加、またはメンバの削除を行います。

構文

config sim [add <candidate_id 1-32> {<password>} | delete <member_id 1-32>]

説明

ID 番号によって SIM グループから CaS の追加、またはメンバの削除を行います。

パラメータ

パラメータ	説明
add <candidate_id 1-32> <password>	CaS を SIM グループの MS 変更します。（必要であれば）、CaS は ID 番号とパスワードによって定義することも可能です。
delete <member_id 1-32>	SIM グループのメンバを削除します。MS は ID 番号によって定義されます。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

メンバを追加します。

```
DES-3526:admin#config sim_group add 2
Command: config sim_group add 2

Please wait for ACK!!!
SIM Config Success !!!

Success.

DES-3526:admin#
```

メンバを削除します。

```
DES-3526:admin#config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK!!!
SIM Config Success!!!

DES-3526:admin#
```

config sim

目的

スイッチの SIM プロトコルの役割パラメータを設定します。

構文

config sim [[commander {group_name <groupname 64>} | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>]]

説明

SIM スイッチのパラメータを設定します。

パラメータ

パラメータ	説明
commander	以下のパラメータで CS を設定します。 • group_name <groupname 64> - グループ名を更新します。64 文字以内の半角英数字の文字列を入力して、SIM グループ名を更新します。
candidate	CS を CaS に変更します。
dp_interval <30-90>	スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔（秒）を設定します。CS スイッチに情報が送られてくると、接続する他のスイッチ（MS、CaS）の情報が CS に組み込まれます。（例 : MS、CaS）。dp_interval は 30-90（秒）の間から指定します。
hold_time <sec 100-255>	他のスイッチが「Discovery Interval」の間隔で送信された情報をスイッチが保持する時間（秒）を指定します。100-255 の間から指定します。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

Discovery プロトコルの間隔を変更します。

```
DES-3526:admin#config sim dp_interval 40
Command: config sim dp_interval 40

Success.

DES-3526:admin#
```

Discovery プロトコルの保持時間を変更します。

```
DES-3526:admin#config sim hold_time 120
Command: config sim hold_time 120

Success.

DES-3526:admin#
```

CS を CaS に移行します。

```
DES-3526:admin#config sim candidate
Command: config sim candidate

Success.

DES-3526:admin#
```

スイッチを CS に移行します。

```
DES-3526:admin#config sim commander
Command: config sim commander

Success.

DES-3526:admin#
```

グループ名を更新します。

```
DES-3526:admin#config sim commander group_name Demetrius
Command: config sim commander group_name Demetrius

Success.

DES-3526:admin#
```

download sim

目的

ファームウェアまたはコンフィグレーションファイルを指定デバイスにダウンロードします。

構文

download sim [firmware | configuration] <ipaddr> <path_filename> {members <mslist> | all}

説明

ファームウェアまたはコンフィグレーションファイルを TFTP サーバから指定デバイスにダウンロードします。

パラメータ

パラメータ	説明
firmware	SIM グループのメンバにファームウェアをダウンロードします。
configuration	SIM グループのメンバにスイッチのコンフィグレーションをダウンロードします。
<ipaddr>	TFTP サーバの IP アドレスを入力します。
<path_filename>	TFTP サーバのファームウェアまたはスイッチのパス名およびファイル名を入力します。
members <mslist> | all	ファームウェアまたはスイッチのコンフィグレーションファイルをダウンロードする先のメンバを指定します。以下のパラメータから 1 つを追加することによって、メンバを指定します。 • <mslist> - 値を入力し、ファームウェアまたはスイッチのコンフィグレーションファイルを受け取る SIM グループのメンバを指定します。 • all - ファームウェアまたはスイッチのコンフィグレーションファイルを SIM グループのすべてのメンバが受け取ります。

制限事項

管理者レベルユーザのみ本コマンドを実行できます。

使用例

ファームウェアをダウンロードします。

```
DES-3526:admin#download sim_ms firmware 10.53.13.94 c:/des3500s.had all
Command: download sim_ms firmware 10.53.13.94 c:/des3500.had all

This device is updating firmware. Please wait...

Download Status :

ID MAC Address       Result
-- ----------------- -------
1  00-01-02-03-04-00 Success
2  00-07-06-05-04-03 Success
3  00-07-06-05-04-03 Success

DES-3526:admin#
```

コンフィグレーションファイルをダウンロードします。

```
DES-3526:admin#download sim configuration 10.53.13.94 c:/des3500.txt all
Command: download sim configuration 10.53.13.94 c:/des3500.txt all

This device is updating configuration.Please wait...

Download Status :

ID MAC Address       Result
-- ----------------- -------
1  00-01-02-03-04-00 Success
2  00-07-06-05-04-03 Success
3  00-07-06-05-04-03 Success

DES-3526:admin#
```

upload sim_ms

目的

SIM グループの指定メンバから TFTP サーバにコンフィグレーションファイルかログファイルをアップロードします。

構文

upload sim_ms [configuration | log] <ipaddr> <path_filename> { [members <mslist 1-32> | all]}

説明

SIM グループの指定メンバから TFTP サーバにコンフィグレーションファイルをアップロードします。

パラメータ

パラメータ	説明
[configuration | log]	アップロードするファイルを選択します。
<ipaddr>	TFTP サーバの IP アドレスを入力します。
<path_filename>	コンフィグレーションファイルをアップロードする TFTP サーバのユーザ定義パスとファイル名を入力します。
[<member_id 1-32> | all]	スイッチコンフィグレーションまたはログファイルをアップロードする先のメンバを指定します。以下のパラメータから 1 つを追加することによって、メンバを指定します。 • <member_id 1-32> - 値を入力し、スイッチのコンフィグレーションファイルまたはログファイルをアップロードする SIM グループのメンバを指定します。 • all - スイッチのコンフィグレーションファイルまたはログファイルを SIM グループのすべてのメンバがアップロードします。

制限事項

管理者レベルおよびオペレータレベルユーザのみ本コマンドを実行できます。

使用例

TFTP サーバにコンフィグレーションファイルをアップロードします。

```
DES-3526:admin#upload sim_ms configuration 10.55.47.1 D:\configuration.txt 1
Command: upload sim_ms configuration 10.55.47.1 D:\configuration.txt 1

This device is upload configuration.Please wait several minutes…

DES-3526:admin#
```

第 37 章　コマンドヒストリリストコマンド

コマンドラインインタフェース（CLI）におけるコマンドヒストリリストコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
?	{<command>}
config command_history	<value 1-40>
show command_history	
dir	

次のセクションで各コマンドについて詳しく説明します。

?

目的

コマンドラインインタフェース（CLI）におけるすべてのコマンドを表示します。

構文

?{<command>}

説明

コマンドラインインタフェース（CLI）を通じ、利用可能なコマンドのすべてを表示します。

パラメータ

パラメータ	説明
{<command>}	適切なコマンドと共に「?」を入力すると、指定コマンドに対応するすべてのパラメータの一覧がコマンド機能の簡単な説明とコマンド内に同じ用語を持つ類似のコマンドと共に表示されます。

制限事項

なし。

使用例

CLI に含まれるすべてのコマンドを表示します。

```
DES-3526:admin#?
..
?
clear
clear arptable
clear counters
clear dhcp_binding
clear fdb
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x capability ports
config 802.1x guest_vlan
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

指定コマンドのパラメータを表示します。

```
DES-3526:admin#config stp
Command: ? config stp

Command: config stp
Usage:{maxage <value 6-40> | maxhops <value1-20> | hellotime <value 1-10> | forwarddelay
<value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | lbd [enable | disable]
| lbd_recover_timer [0 | <value 60-1000000>]}
Description:Used to update the STP Global Configuration.
config stp instance_id
config stp mst_config_id
config stp mst_ports
config stp ports
config stp priority
config stp version

DES-3526:admin#
```

config command_history

目的

コマンドヒストリを設定します。

構文

config command_history <value 1-40>

説明

コマンドヒストリを設定します。

パラメータ

パラメータ	説明
<value 1-40>	バッファに保持されている過去に実行したコマンド数。最新の実行されたコマンドを最大 40 個まで参照することができます。

制限事項

なし。

使用例

コマンドヒストリを設定します。

```
DES-3526:admin#config command_history 20
Command: config command_history 20

Success.

DES-3526:admin#
```

show command_history

目的

コマンドヒストリを表示します。

構文

show command_history

説明

コマンドヒストリを表示します。

パラメータ

なし。

制限事項

なし。

使用例

コマンドヒストリを表示します。

```
DES-3526:admin#show command_history
Command: show command_history

?
?show
show vlan
show coomand history

DES-3526:admin#
```

dir

目的

コマンドラインインターフェイス上のコマンドをすべて表示します。

構文

dir

説明

コマンドラインインターフェイス上のコマンドをすべて表示します。

パラメータ

なし。

制限事項

なし。

使用例

コマンドを表示します。

```
DES-3526:admin#dir
Command: dir

..
?
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear dhcp binding
clear dhcp conflict_ip
clear fdb
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config accounting type
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```